UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

KRIPTOGRAFIJA in VARNOST SLOVENSKIH E-TRGOVIN

Ljubljana, april 2006 **ROK SABADIN**

IZJAVA

Študent Rok Sabadin izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Andreja Kovačiča in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 06. 04. 2006 Podpis:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

KAZALO TABEL V PRILOGI

1. UVOD

Danes si težko predstavljamo življenje brez mobilnega telefona ali interneta z neskončnim pretokom informacij. Govorimo o informacijski družbi, ki jo ustvarja revolucija na področju informacijske tehnologije. Tehnologija se je v zadnjih tridesetih letih bliskovito razvijala in pogosto je bilo vprašanje varnosti zapostavljeno. Z obdobjem rasti elektronske komunikacije in izmenjavo občutljivih informacij postane varnost ključna kategorija. Dejstvo je, da elektronsko poslovanje v marsičem presega meje organizacije in informacijsko varnost lahko zagotovimo le z zahtevnimi šifrirnimi mehanizmi.

Namen magistrskega dela je pregled tuje in domače literature s področja kriptografije. Dostopno je večje število strokovnih člankov, ki so omejeni na posamezno rešitev, njihovo razumevanje pa je pogojeno z dobrim poznavanjem osnov kriptografije. Abecednik na področju kriptografije v slovenskem jeziku tako rekoč ne obstaja. Namen je napisati delo, ki bo bralca postopoma vpeljalo v kompleksni svet kriptografije, začenši z osnovami in postopnimi nadgraditvami vse do matematičnih izračunov. Na podlagi teoretičnih spoznanj bomo razvili metodo ocenjevanja varnosti spletnih trgovin, ki jo bomo uporabili v empiričnem delu naloge. V Sloveniji ne beležimo raziskav s področja varnosti nakupov preko interneta, kljub temu da je to področje ključnega pomena za zagotavljanje zaupanja potrošnikov in s tem dolgoročnega obstoja podjetja. Raziskava evropskega statističnega urada Eurostat, Uporaba interneta v Evropi s poudarkom na varnosti in zaupanju, navaja relativno majhno število uporabnikov, ki so imeli težave pri nakupovanju preko interneta. Kljub temu velja izpostaviti problem pomanjkljive varnosti plačevanja, kjer se je Slovenija uvrstila na neslavno prvo mesto (3,7 % kupcev je zaznalo pomanjkljivo varnost pri plačevanju preko interneta). V empiričnem delu naloge bomo analizirali varnost nakupovanja v slovenskih spletnih trgovinah. Vsako spletno trgovino bomo obiskali in simulirali nakup naključno izbranega izdelka vse do potrditve nakupa. Na koncu bomo predlagali rešitve za zagotavljanje ustrezne ravni varnosti.

Temeljna hipoteza magistrskega dela: *Mnoge slovenske spletne trgovine nimajo vgrajenih ustreznih varnostnih protokolov za zagotavljanje varnega nakupovanja preko interneta.*

Metoda magistrskega dela temelji na teoretičnem pregledu slovenske in tuje literature s področja kriptografije. V empiričnem delu je uporabljena metoda analize posamezne spletne trgovine, ki je ocenjena v skladu z metodo ocenjevanja varnosti spletnih trgovin. Rezultati analize so interpretirani s pomočjo deskriptivne statistike.

Vsebinsko je magistrsko delo razdeljeno na sedem poglavij. Prvo poglavje je namenjeno opredelitvi osnovnih pojmov in nas vpelje v svet interneta, elektronskega poslovanja in informacijske varnosti. Drugo poglavje predstavlja osnove kriptografije vse od zgodovine do

različnih tehnik šifriranja. Pridobimo osnovno znanje in razumevanje, ki ga v tretjem poglavju nadgradimo z razlago simetričnih in asimetričnih algoritmov v praksi. Današnje varnostne rešitve so zelo kompleksne in ne vsebujejo samo enega algoritma. Rešitve, sestavljene iz vrste različnih algoritmov, imenujemo programi oziroma protokoli, ki zagotavljajo celovito varnostno rešitev in so opisani v četrtem poglavju. Sledi poglavje s praktičnimi napotki in metodo ocenjevanja varnosti spletnih trgovin, ki bi utegnili zanimati tudi naključnega bralca. Večino magistrskega dela predstavljajo zahtevni algoritmi, ki so sicer uporabljeni v praksi, vendar povprečnemu bralcu ne prinašajo dodane vrednosti v smislu lastne varnosti. Poglavje nas nauči, kako varno nakupovati preko interneta, varno pošiljati elektronsko pošto in shranjevati podatke na lokalnem disku v šifrirani obliki. Šesto poglavje zaokrožuje empirični del magistrske naloge, ki analizira varnost slovenskih e-trgovin. Zadnje poglavje se ukvarja s stroškovnim vidikom vzpostavitve prave (varne) e-trgovine.

2. OSNOVNI POJMI

2.1 Internet

Sovjetska zveza je konec leta 1957 v vesolje izstrelila satelit Sputnik. Kot odgovor je čez nekaj mesecev ameriški oddelek za varnost na pobudo predsednika Dwighta D. Eisenhowerja ustanovil agencijo za napredne raziskovalne projekte (ARPA - Advanced Research Projects Agency), ki je zaposlila nekaj najbolj naprednih ljudi tedanjega časa. Že po poldrugem letu so predstavili prvi ameriški satelit. Kasneje se je agencija ARPA začela ukvarjati z naprednimi računalniškimi tehnologijami in leta 1969 predstavi prvo distribuirano računalniško mrežo, ki omogoča komunikacijo med dislociranimi uporabniki v primeru vojaškega napada. Mreža se je imenovala ARPANET in je omogočala izmenjavo podatkov v paketih (Gromov, 2005).

ARPANET je bil primarno vojaški projekt, vendar je že v začetku omogočal izmenjavo informacij med izbranimi univerzami in raziskovalnimi laboratoriji. Kasneje se je razširil na komercialne množice in tako je nastal internet.

Internet je mreža tisočih računalniških mrež, ki so dostopne milijonom uporabnikov po vsem svetu. Kot komunikacijski medij se je zaradi svoje hitrosti in učinkovitosti zelo razširil in je v marsičem presegel svojo prvotno misijo. Uporabljajo ga mnogi ljudje in organizacije – časopisi, založniki, televizijske postaje, učitelji, knjižničarji, poslovni ljudje itd. – za različne namene. Internet ni zgolj množica računalnikov, je mnogo več, je kibernetski prostor, ki omogoča komuniciranje in poslovanje 24 ur na dan kjerkoli na tem svetu (LaQuey, 1994). Eksponentno rast interneta nazorno prikaže podatek, da so bili leta 1969 v mrežo povezani štirje gostitelji, konec leta 2004 pa že preko 285 milijonov gostiteljev (Zakon, 2005).

Pogosto pravimo, da je denar sveta vladar in v svojo mrežo je ujel tudi internet, ki omogoča pravo elektronsko poslovanje.

2.2 Elektronsko poslovanje

Elektronsko poslovanje je s povezovanjem računalnikov in interneta v marsičem spremenilo naš vsakdanjik. Razvoj tehnologij je nepričakovano povečal obseg elektronskega poslovanja, ki prinaša koristi tako prodajalcem kot kupcem, enim v obliki izjemno velikega trga, drugim v obliki nižjih cen in večje konkurence. Elektronsko poslovanje definiramo kot uporabo komunikacijskih medijev za kupovanje in prodajanje izdelkov ali storitev, ki potrebujejo fizični ali digitalni transport iz ene lokacije do druge (Greenstein et al., 1999).

Elektronsko poslovanje omogoča podjetjem doseganje večjih dobičkov, kupcem pa nižje cene. Podjetje lahko ponudi nižje cene, ker ni potrebe po dragih poslovnih prostorih in skladiščih v središčih mest, kjer je gostota potencialnih kupcev najvišja. Poleg tega ne potrebujejo drage delovne sile, ker je večina procesov avtomatiziranih. Korak naprej predstavlja globalizacija in z njo prisotnost na pomembnejših svetovnih trgih. Vstop na tuji trg pogosto predstavlja pomembno stroškovno postavko pri poslovanju. Veliko sredstev je potrebno vložiti v oglaševanje, nove poslovne prostore, delovno silo itd. V nasprotju s tem poslovanje preko interneta omogoča vstop na tuje trge z minimalnimi stroški (Griffin et al., 2002). Elektronsko poslovanje dodaja novo vrednost v obliki večje prilagodljivosti, saj kupcu omogoča prilagoditev izdelka z možnostjo velikega nabora različnih značilnosti in opcij.

Navkljub dejstvu, da ima elektronsko poslovanje mnoge prednosti, je njegova uporaba v praksi daleč od popolne. Pojavi se vprašanje zasebnosti in zaščite podatkov, ki se pretakajo preko interneta.

2.3 Informacijska varnost

Podjetja se v današnjem poslovnem okolju soočajo z zahtevnim izzivom ohranjanja konkurenčnosti. S ciljem racionalizacije stroškov in približevanja kupcu prilagajajo obstoječo informacijsko infrastrukturo, s čimer odpirajo vrata svojega sistema. V tej točki se pojavi vprašanje informacijske varnosti, ki zajema zaščito podatkov in fizičnih komponent sistema pred nenamerno ali namerno zlorabo. Najpogosteje izvirajo iz raznih prevar, kraj storitev, intelektualne lastnine, privatnih podatkov ter vsakdanjega vandalizma (Gordon et al., 2004).

Mnoga podjetja razmišljajo v duhu »nam se to ne more zgoditi«, vendar spregledajo dejstvo, da lahko tudi računalniki brez pomembnejše vsebine omogočajo nepridipravom podlago za napade na druge računalniške sisteme (Houle et al., 2001). Zanimivo je, da utegnejo biti podjetja, ki za svoje računalnike in mreže ne skrbijo z vestnostjo dobrega gospodarja, pravno

formalno odgovorna za škodo, ki je preko njihovega sistema povzročena drugim podjetjem (Greene, 2000). Mnoga podjetja o varnosti razmišljajo kot o kategoriji, ki bo dodana, ko bodo imeli čas ali ko bodo to storitev uporabniki pripravljeni plačati (Acar et al., 2002).

Vendar lahko pogledamo na problem z drugega zornega kota in ugotovimo, da je za dolgoročni obstoj podjetja ključno zaupanje potrošnikov in dobaviteljev. Posledično si podjetja s svojo malomarnostjo ne bi smela privoščiti izgube zaupanja. Raziskava Giga Information Group ugotavlja, da je zaupanje uporabnikov ključna kategorija, ki odloča o uspehu ali neuspehu posamezne spletne storitve. Res je tudi, da popolne varnosti ni. Vprašanje je, do katere mere zaščititi sistem, kajti več ni nujno bolje. Z naraščanjem števila varnostnih ukrepov hitro pada verjetnost zlorabe, vendar prav tako hitro (eksponentno) narašča težavnost uporabe sistema (Eckel et al., 1996). Tako vstopimo v krog varnosti, stroškov in enostavnosti uporabe ter iščemo kompromise.

Strokovnjaki za informacijsko varnost se strinjajo, da je potrebno pri elektronskem poslovanju zadostiti naslednjim varnostnim zahtevam:

- Zaupnost podatkov. Pošiljanje podatkov mora biti tako zaščiteno, da je vsebina skrbno varovana, pošiljatelja in prejemnika sporočila pa ni možno identificirati.

- Neokrnjenost podatkov. Podatki, poslani v elektronski obliki, se med prenosom ne smejo popačiti, izgubiti ali kako drugače spremeniti.

- Razpoložljivost. Komunikacijska infrastruktura in računalniška mreža morata permanentno omogočati pošiljanje in sprejemanje podatkov, kar je pogoj za izvajanje elektronskega poslovanja.

- Pristnost. Pri pošiljanju sporočila moramo biti prepričani, da bo poslano točno določenemu naslovniku. Prav tako mora biti naslovnik prepričan, da je sporočilo poslal točno določen pošiljatelj in ne kakšna tretja oseba (Lawrence et al., 2000).

- Nezanikanje. Sistem mora zagotavljati, da niti pošiljatelj niti prejemnik ne moreta zanikati pošiljanja oziroma prejema sporočila (Stallings, 1995).

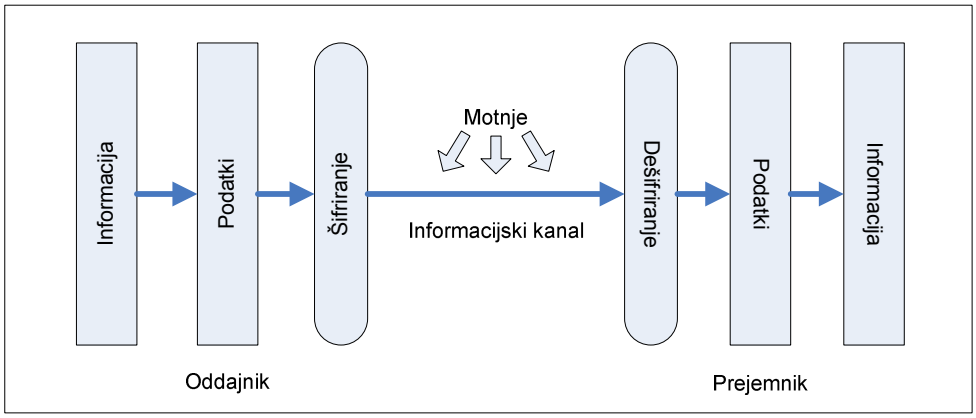
Varnost lokalnih sistemov je mogoče doseči s fizičnimi varnostnimi ukrepi, kar je razmeroma enostavno. Korak naprej predstavlja elektronsko poslovanje, ki v marsičem presega meje organizacije. V takšnih in podobnih primerih si pri zagotavljanju informacijske varnosti pomagamo z zahtevnimi kriptografskimi mehanizmi.

2.4 Osnove komuniciranja

Jedro komuniciranja je informacija. Poleg informacije potrebujemo nekoga, ki informacijo pripravi in odda ter tistega, ki mu je informacija namenjena in jo prejme.

Tako imamo 3 bistvene sestavine komuniciranja: oddajnika, informacijo in prejemnika. Komuniciranje je torej prenos informacij od oddajnika k prejemniku. Oddajnik mora informacijo šifrirati v obliko, primerno za prenos, jo po informacijskem kanalu poslati prejemniku, ki jo nato dešifrira (Wechtersbach et al., 1997). Na informacijski kanal delujejo motnje, zaradi katerih se lahko oddani signal izgubi, popači ali kako drugače preoblikuje in prejemnik poslanega signala ne razume več (slika 2.1).

Slika 2.1: Osnovni model komuniciranja



Vir: Wechtersbach et al., 1997, str. 51

Cilj komuniciranja je torej prenesti informacijo od oddajnika k prejemniku. Toda to je zgolj delni in ne končni cilj. Bistven namen komuniciranja je spremeniti obstoječe stanje pri prejemniku. S posredovano informacijo želimo vplivati na prejemnika, ga osveščati, informirati, prepričati itn. Na primer, prijatelj si želi kosila in mi mu podamo informacijo, kje se nahaja dobra gostilna. S tem smo ga informirali, mu olajšali izbiro ter posredno bolje zadovoljili njegove potrebe.

Informacijo lahko sporočamo prejemniku preko različnih informacijskih kanalov (ustno, pisno, preko telefona, računalnika itn.). Kadar komunicirajo ljudje, ki niso v neposrednem stiku, je potrebno komunikacijski kanal dopolniti z raznimi tehničnimi pripomočki, ki omogočajo prenos sporočila oziroma podatkov na večjo razdaljo. V ta namen uporabljamo različna telekomunikacijska omrežja.

3. KRIPTOGRAFIJA

3.1 Zgodovina kriptografije

Zgodovina kriptografije sega v dobo približno 2000 let pred našim štetjem, ko so Egipčani s pomočjo hieroglifov krasili grobove. Namen ni bil prikrivanje informacij, temveč veličasten in svečan opis življenja pokojnika. Kasneje so civilizacije Egipčanov, Hebrejcev in Sirijcev nadalje razvijale svoje kriptografske sisteme. Obstaja mnogo skrivnostnih zapisov, vklesanih v kamnite plošče in napisanih na papirus. Sklepamo lahko, da so zaradi takšnega ali drugačnega razloga želeli napisano informacijo prikriti.

Prvo zabeleženo uporabo kriptografije z namenom prikrivanja informacij pripisujemo Hebrejcem, ki so razvili šifriranje, imenovano »atbash«. Princip šifriranja je temeljil na zamenjavi črk (Miller, 2005).

Okoli leta 400 pred našim štetjem so Špartanci uporabljali palico, ki so jo razpolovili (slika 3.1). Eno polovico je zadržal pošiljatelj, drugo pa prejemnik sporočila. Pošiljatelj je palico ovil z usnjenim trakom, na katerega je napisal sporočilo. Nato je trak odvil in ga poslal prejemniku. Slednji je trak ovil na palico enakega premera in tako dobil berljivo sporočilo. Omenjeni način šifriranja podatkov so uporabljali za pošiljanje vojaških napotkov (Ekert, 2005).

Slika 3.1: Primer špartanske kriptografije

VIR: http://global.mitsubishielectric.com/misty, 2005

Kasneje v zgodovini je Julij Cezar razvil metodo šifriranja, podobno »atbashu«. Vsako črko berljivega besedila je spremenil s črko tri mesta naprej v abecedi. Tako je dobil šifrirano sporočilo, ki sicer ne zagotavlja velike varnosti, toda v tistem času so znali brati le redki posamezniki in še te je bilo možno hitro zmesti. Razvoj tehnik šifriranja se je iz leta v leto izboljševal in je bil primarno namenjen vojaški komunikaciji.

Uporaba kriptografije v Evropi se je razširila v srednjem veku. Razvoj je bil opazen predvsem v mestih po Italiji. Okoli leta 1379 je Gabriele de Lavinde iz Parme, ki je bil v službi Papeža Clementa VII, napisal prvi evropski priročnik o kriptografiji. Vseboval je nabor ključev, ki so predvidevali uporabo unikatnih simbolov za določene besede in imena. Leta 1470 Leon Battista Alberti predstavi šifrirni disk in čez dobrih sto let sledi predstavitev kvadratne tabele avtorja Blaise de Vigenere, ki vpeljuje novodobni koncept, pri katerem je algoritem javno poznan, ključ pa mora biti skrbno varovan (Ekert, 2005).

Med drugo svetovno vojno pride do velikega napredka z uporabo mehaničnih in elektromehaničnih tehnologij. Verjetno najbolj znana tehnična naprava za šifriranje in dešifriranje je bila razvita med drugo svetovno vojno v Nemčiji in se je imenovala Enigma (slika 3.2). Na prvi pogled je spominjala na pisalni stroj s tremi do petimi kolesi (rotorji), ki jih je bilo možno poljubno nastavljati. Operator je natipkal sporočilo, ki ga je Enigma šifrirala v skladu z nastavitvami koles.

Slika 3.2: Enigma – naprava za šifriranje in dešifriranje

VIR: http://www.mccullagh.org, 2005

Šifrirano sporočilo so nato poslali naslovniku, ki je na osnovi poznavanja pošiljateljevih nastavitev koles opravil proces dešifriranja. Nacisti so bili prepričani, da Enigma zagotavlja popolno varnost. Tehnologijo so uporabljali za vse možne komunikacije, med drugim tudi za

komunikacije med svojimi tajnimi službami. Britanci so se zavedali nevarnosti in so v skrbno varovani projekt Ultra, katerega namen je bil razvozlati Enigmo, vložili veliko sredstev. Dešifriranje Enigme je bilo zelo zahtevno, vendar jim je na koncu le uspelo. Ugotovili so, kako deluje, vendar so za dešifriranje potrebovali vnaprej dogovorjeno listo nastavitev koles (ključ). Pravilno so sklepali, da nemške ladje s seboj prevažajo knjigo nastavitev za daljše obdobje in z napadi so prišli do dragocenih informacij. Leta 1941 so projekt prvič upravičili z dešifriranjem sporočil, ki so govorila o nemški invaziji na Grčijo. Ultra je najpomembnejšo vlogo odigrala pri dešifriranju sporočil o lokacijah nemških podmornic v severnem Atlantiku. Le tako so se lahko zavezniški konvoji tovornih ladij izognili nevarnosti. Kasneje so nacisti Enigmo izboljšali in Britanci so potrebovali nadaljnjega pol leta za razkritje njenega delovanja. Menda je rešitev uganke, imenovane Enigma, skrajšala drugo svetovno vojno za dve leti (Lycett, 2001).

Z razvojem zmogljivih računalnikov so se kriptografske tehnike izjemno izboljšale. V novejši zgodovini je poznan uspešen IBM-ov projekt Lucifer, ki je leta 1974 v kriptografijo vpeljal 128-bitni ključ in zahtevne matematične algoritme. Slednje je kasneje prevzela in nadgradila agencija NSA (U.S. National Security Agency) ter predstavila standard DES (Data Encryption Standard), ki je bil v uporabi preko 25 let (Bamford, 1983).

Naslednja velika revolucija se je pričela z razvojem mikroprocesorskih računalnikov, ki so naprednemu uporabniku omogočali vdore v večino obstoječih algoritmov. Posledično je prišlo do razvoja zelo zahtevnih algoritmov kot na primer Rijndaela ali kriptografije eliptičnih krivulj (Harris, 2001).

3.2 Osnove kriptografije

Namen poglavja je razložiti osnovne pojme kriptografije. Bralec bo kmalu spoznal, da beseda kriptografija ni tako strašna, kot zgleda na prvi pogled. Kriptografija izhaja iz dveh grških besed: kryptos (κρνπτοσ) in graphia (γραφια). Prva pomeni skrivati, druga pa pisati (Hipschman, 1995). Neposreden prevod bi lahko bil »tajnopisje«.

Slovar slovenskega knjižnega jezika sicer ne opredeljuje pojma kriptografija, temveč opredeli *šifro* kot dogovorjen znak iz ene ali več črk ali števk, ki se uporablja za ohranitev tajnosti sporočila. Glagol *šifrirati* pomeni spreminjati v šifre, medtem ko *dešifrirati* pomeni razbrati s šiframi napisano besedilo.

Kriptografija je mnogo več kot le tajnopisje. Izrazito je povezana z vprašanjem varnosti in omogoča, da lahko varno poslujemo preko interneta, da geslo za dostop do pomembnih vsebin ni zlorabljeno, da prejemnik elektronske pošte ve, da smo mu jo poslali prav mi in nenazadnje, da lahko z uporabo kreditne kartice kupujemo na internetu. Obstajajo algoritmi, ki so zelo

enostavni in ne zagotavljajo velike varnosti, ter tisti, ki so zelo zahtevni in varni. Kot ponavadi je velika večina algoritmov nekje vmes, v zlati sredini. Pomembna je ugotovitev, da popolne zaščite ni. Večino algoritmov je možno »razbiti«, pogoj je le, da ima nepridiprav dovolj časa, volje in sredstev. Zaključimo, da cilj kriptografije ni popolna ampak relativna zaščita. To pomeni, da je raven zaščite odvisna od pomembnosti zaščitenih informacij in da mora biti »razbitje« šifre v vsaki točki dražje od vrednosti pridobljenih informacij.

V zgodovini so proces šifriranja izvajali ročno, danes si pomagamo z računalniki. V samem bistvu se šifriranje ni spremenilo, le implementacija, kompleksnost in hitrost so izboljšane.

3.2.1 Berljivo in šifrirano sporočilo

Vsakodnevna komunikacija poteka v jeziku, ki jo s predpostavko poznavanja jezika razumemo vsi. Sporočilo je sicer namenjeno ciljni skupini ali posamezniku, vendar ga lahko prestrežejo in razumejo tudi tretje osebe. Dober primer je naročanje hrane in pijače v restavraciji. Naše sporočilo je namenjeno natakarju, toda sporočilo lahko razumejo vsi navzoči. Enako velja za komunikacijo s pomočjo elektronske pošte. Besedilo pišemo v razumljivem jeziku. Recimo, da Rok pošlje sporočilo Katji.

Živijo, Katja.

Včeraj sem govoril z gospodom Črnkom in zgleda, da bo prišlo do prevzema. To je enkratna priložnost. Kupi delnice Kriptkoma!

Lp Rok

Čeprav je očitno, da je sporočilo namenjeno Katji, ga lahko prestreže tretja oseba in s tem pridobi zaupne informacije. Imamo opravka z berljivim tekstom, ki ni šifriran in ga lahko razume pošiljatelj, prejemnik in druge nepooblaščene osebe, ki imajo dostop do sporočila. V vsakdanji komunikaciji se ne obremenjujemo z dejstvom, da nas poslušajo navzoči, ker v takšnih situacijah ne govorimo o svojih skrivnostih.

Če želimo, da sporočilo ostane skrivnost oziroma da ga razumeta le pošiljatelj Rok in prejemnica Katja, lahko uporabimo enostavno šifriranje - vsako črko sporočila zamenjamo s črko, ki je tri mesta naprej v abecedi. Torej A zamenjamo s Č, B z D, C z E in tako naprej. Primer šifriranega sporočila namenjenega Katji.

Clalms Nčzmč.

Afhtčm uhp jsastlo b jsušsgsp Ftrnsp lr bjohgč, gč ds štlvos gs šthabhpč. Zs mh hrntčzrč štloscrsuz. Nžšl ghorleh Ntlšzspč!

Oš Tsn

V zgornjem primeru smo vsako črko abecede zamenjali s črko tri mesta naprej, kar ni pravilo. Lahko izberemo poljubni korak, torej zamenjamo črko s črko za štiri, pet ali več mest naprej. Prikrito sporočilo imenujemo šifriran tekst.

Omenjeno shemo šifriranja je uporabljal Julij Cezar in se po njemu imenuje »Cezarjeva šifra«, ki jo uvrščamo v kategorijo ***substitucijskih tehnik šifriranja***. To pomeni, da v procesu šifriranja vsako črko berljivega teksta zamenjamo z določeno drugo črko, številom ali simbolom, pri čemer ostaja vrstni red črk znotraj besede nespremenjen (Wrixon, 2000). Takšen način šifriranja je zelo enostaven, kar posledično vpliva na relativno majhno varnost.

Glavna pomanjkljivost Cezarjeve šifre je njena predvidljivost. V najslabšem primeru moramo poizkusiti 24 alternativ in uspeh je zagotovljen. Predstavljajte si, da uporabimo naključno substitucijo. To pomeni, da črko A zamenjamo s poljubno črko v abecedi, enako naredimo s črko B in tako naprej. Bistveno pri tem je, da zamenjava črke A s poljubno črko nima nikakršne povezave z zamenjavo črke B s poljubno črko. V dobi pred našim štetjem bi bila takšna kriptografija izredno učinkovita.

Pri nepooblaščenem dešifriranju si lahko pomagamo s poznavanjem jezika in pogostosti pojavljanja posameznik črk v besedilu. Slovenski jezikoslovci so na podlagi analize določili verjetnost pojavljanja posameznih črk: E (7,92 %), A (7,74 %), O (6,72 %), I (6,69 %) in tako dalje. Napadalec s pomočjo poznavanja pogostosti pojavljanja črk statistično analizira šifriran tekst in poskuša s pomočjo poskusov in napak vdreti vanj (Jakopin, 1999).

Poleg substitucijskih poznamo še ***transpozicijske tehnike šifriranja***, ki črke sporočila prestavljajo, ne da bi jih zamenjale z drugo črko, številom ali simbolom. Primer takšne tehnike so anagrami oziroma premetanke, ki črke besede prerazporedijo in tako oblikujejo novo besedo (npr. besedo *mentor* spremenimo v *monter*). Za razumevanje transpozicijskega šifriranja predstavljamo tehniko transpozicije v stolpcih. V poljubno veliko tabelo pišemo sporočilo v vrsticah (tabela 3.1). Začnemo v prvi vrstici in nadaljujemo v drugi in tako dalje. Šifriran tekst dobimo tako, da šifrirano sporočilo beremo v stolpcih od zgoraj navzdol. Lahko začnemo brati v prvem stolpcu, lahko pa izberemo poljubni vrstni red in tako še dodatno otežimo razumevanje sporočila. Napišimo *kupi delnice* v dveh vrsticah. Začnemo v prvi in nadaljujemo v drugi.

Tabela 3.1: Transpozicijska tehnika šifriranja

Stolpec 1	Stolpec 2	Stolpec 3	Stolpec 4	Stolpec 5	Stolpec 6
K	U	P	I	D	E
L	N	I	C	E	

Vir: Cherowitzo, 2005

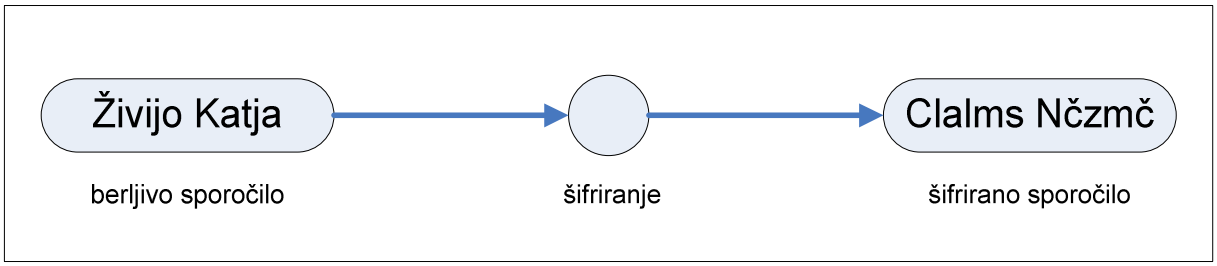
Šifrirano sporočilo beremo v stolpcih (na primer od leve proti desni) *KLUNPIICDEE*. Lahko se odločimo in beremo v stolpcih po sledečem vrstnem redu 5,4,2,1,3,6 in dobimo šifrirano sporočilo *DEICUNKLPIE*. Zaščita ni kdo ve kako močna in razbitje šifre je vprašanje nekaj kombinacij in poskusov. Lahko pa omenjeno tehniko izpopolnimo z dodajanjem več krogov, ki povečujejo varnost šifriranega sporočila.

Posamezne tehnike, tako substitucijske kot transpozicijske, niso dovolj varne. Veliko višjo raven varnosti zagotavljamo s prepletanjem obeh, kar predstavlja most med klasičnimi in modernimi oblikami šifriranja.

3.2.2 Šifriranje in dešifriranje sporočila

Zgoraj smo predstavili koncept spreminjanja berljivega sporočila v šifrirano sporočilo z namenom prikrivanja vsebine nepooblaščenim osebam. Proces spremembe berljivega sporočila v neberljivo imenujemo šifriranje (slika 3.3).

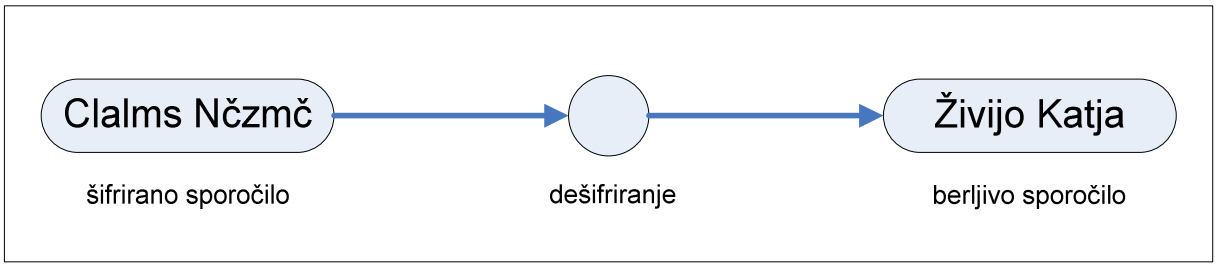
Slika 3.3: Šifriranje



Vir: Chapple, 2003

Obraten proces, ko želi prejemnik spremeniti šifrirano sporočilo v razumljivo obliko, imenujemo dešifriranje, ki je prikazano v sliki 3.4.

Slika 3.4: Dešifriranje

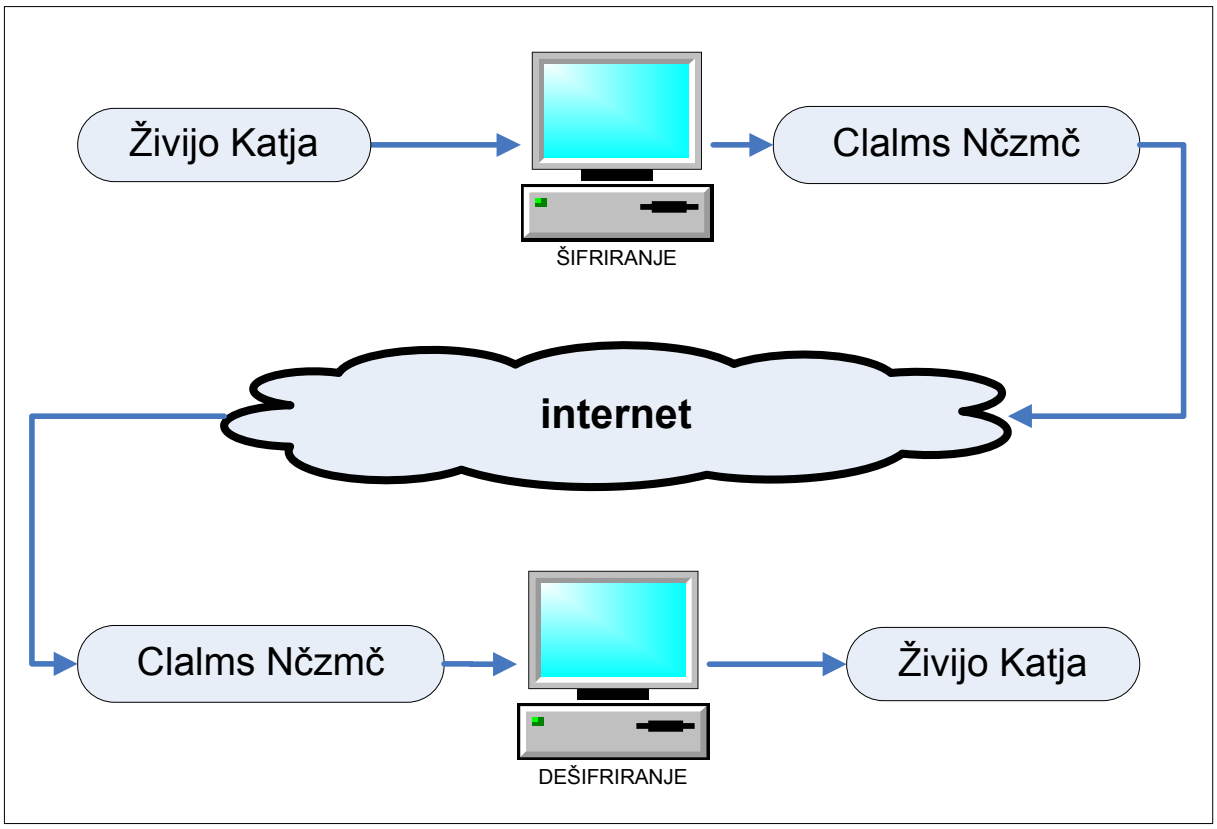


Vir: Chapple, 2003

Na podoben način poteka komunikacija med različnimi računalniki v omrežju oziroma internetu. Uporabnik natipka sporočilo, ki ga računalnik šifrira in pošlje po komunikacijskem

kanalu. Prejemnikov računalnik opravi proces dešifriranja in prikaže sporočilo v uporabniku razumljivi obliki (slika 3.5). Komunikacija je uspešna le, če oba udeležena računalnika uporabljata enak algoritem, prvi za šifriranje, drugi za dešifriranje. To pomeni, da se morata pošiljatelj in prejemnik dogovoriti o uporabi enakega algoritma.

Slika 3.5: Šifriranje in dešifriranje v računalniški komunikaciji



Vir: http://shiflett.org/images/18fig01.jpg, 2005

Proces šifriranja in dešifriranja sestavljata dva pomembna elementa: algoritem in ključ, ki skupaj tvorita unikaten postopek. Algoritem pomeni dogovorjeni postopek (splošno znan), ključ pa predstavlja tisti dodatek, ki naredi postopek unikaten in je poznan samo pošiljatelju in prejemniku sporočila (Chapple, 2003). Na primer sporočilo šifriramo s Cezarjevo šifro. Splošno znano je, da Cezarjeva šifra pomeni zamenjavo črke s črko, ki je nekaj mest naprej (ponavadi 3). Predpostavimo, da se prijatelja dogovorita za šifrirano komunikacijo z zamikom 7 črk. V tem primeru je Cezarjeva šifra algoritem, število 7 pa ključ. Poenostavljeno lahko rečemo, da ključ vstavimo v algoritem in berljivo sporočilo spremenimo v šifrirano. Zaključimo, da predstavlja algoritem nabor možnih matematičnih funkcij, ki jih uporabljamo za modificiranje berljivega sporočila, ključ pa pove v kakšnem vrstnem redu in kako se bodo izvajale, s čimer zagotavljamo unikatnost postopka. Pomembno je, da je nabor možnih ključev dovolj velik, kar neposredno vpliva na varnost šifriranja. Večji kot je nabor ključev, večja je

varnost sistema in obratno. Najšibkejši člen kriptografske verige je prav ključ in ohranjanje njegove tajnosti (Coles, 2005).

Na najvišji ravni delimo kriptografske sisteme na simetrične in asimetrične. Simetrični uporabljajo za šifriranje in dešifriranje enak ključ, medtem ko asimetrični uporabljajo dva različna ključa, enega za šifriranje in drugega za dešifriranje.

3.3 Simetrična kriptografija

V simetričnem kriptografskem sistemu uporabljamo enak ključ za šifriranje in dešifriranje sporočil (slika 3.6). Simetričen ključ, ki se uporablja na obeh straneh procesa, pogosto imenujemo enojni oziroma tajni ključ. Sistem temelji na zaupanju posameznikoma, da skrbno varujeta svoj ključ (Barkley, 1994).

Slika 3.6: Simetrično šifriranje

Vir: Jerman Blažič et al., 2001, str. 103

Na praktičnem primeru bomo skušali razložiti problem varnosti in izmenjave ključev pri simetrični kriptografiji. Imamo dva prijatelja, ki želita izmenjati strogo zaupno pošto in se iz takšnega ali drugačnega razloga ne želita srečati. Najbolj enostavno bi bilo poslati pošto preko navadnega poštarja ali posrednika. Toda ali smo popolnoma prepričani, da posrednik ne bo videl zaupne vsebine? Lahko uporabljamo pečate in plombe, vendar s tem varnost ni zagotovljena. Obstaja druga možnost, in sicer da pošiljatelj sporočilo shrani v kovinsko škatlo s ključavnico. Tako bo prepričan, da je med transportom vsebina skrbno varovana. Žal pa je skrbno varovana tudi pred naslovnikom, ki potrebuje enak ključ kot pošiljatelj. Pojavi se vprašanje izmenjave ključev. Nobenega smisla nima, da ključ potuje skupaj s škatlo. Po drugi strani lahko osebi osebno izmenjata ključ, toda v tem primeru bi si raje izmenjala pismi. Nastopi t. i. problem izmenjave ključev pri simetrični kriptografiji, ki predvideva uporabo enakega ključa za zaklepanje in odklepanje. Če zadevo nekoliko zakompliciramo in si zamislimo nekaj sto prijateljev, bi od vsakega potrebovali unikaten ključ. V nepreglednem šopu ključev bi potrebovali cel dan, da bi našli pravega.

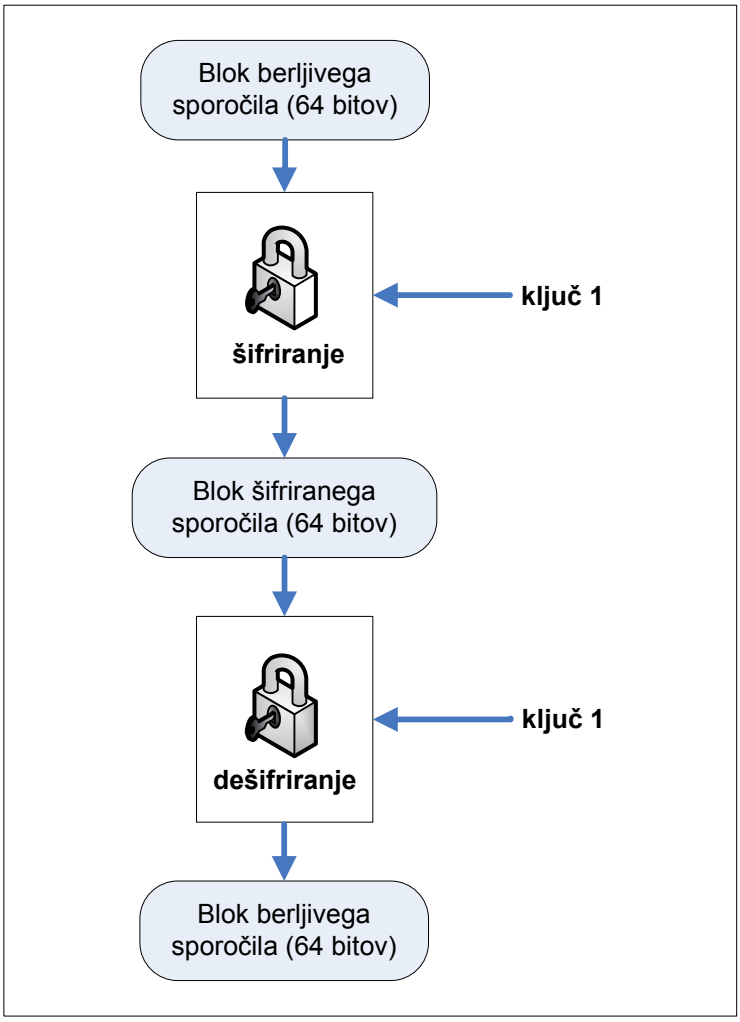
Lahko si predstavljamo 20-kotnik (dvajset uporabnikov) in vse možne povezave med njimi, ki predstavljajo unikatne ključe. Prostor okoli uporabnika postane precej zapolnjen že pri

relativno majhnem številu. Število diagonal je 170 in če prištejemo še 20 medsebojnih povezav, govorimo o 190 unikatnih ključih.

3.3.1 Delitev na blokovne in tokovne tehnike

Tehnike simetrične kriptografije delujejo bodisi na osnovi zamenjav bitov (tokovna kriptografija) bodisi na osnovi zamenjav celotnih blokov berljivega oziroma šifriranega teksta (blokovna kriptografija). ***Blokovna kriptografija*** razdeli sporočilo na fiksne bloke bitov, ki jih s pomočjo substitucij in transpozicij enega po enega spremeni v šifriran tekst (slika 3.7). Algoritem vsebuje nabor možnih funkcij, ki jih izvajamo na bloku sporočila, ključ pa pove, katere funkcije in v katerem vrstnem redu bomo uporabili. Takšen način šifriranja in dešifriranja vsebuje elemente zmešnjave in razpršitve. Zmešnjavo povzročajo različne neznane vrednosti ključev, razpršitev pa omogoča velik nabor možnih funkcij in odvisnost od predhodno šifriranih blokov (Khalili, 2005).

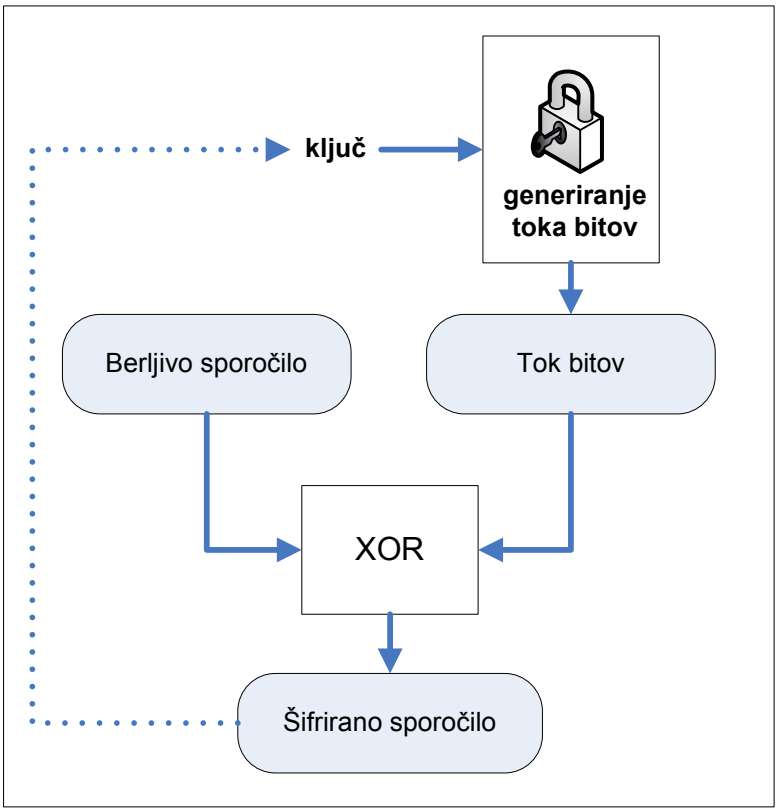
Slika 3.7: Blokovna kriptografija



Vir: Jutla, 2005

Poleg blokovne poznamo ***tokovno kriptografijo***, ki ne razdeli sporočila na bloke, temveč obravnava sporočilo kot tok osnovnih gradnikov (bitov), na katerih individualno izvaja matematične funkcije (slika 3.8). Ker deluje na nivoju bita, je bolj primerna za strojne rešitve in sodi v silicijevo okolje, nasprotno je blokovna kriptografija primernejša za programske rešitve (Khalili, 2005).

Slika 3.8: Tokovna kriptografija



Vir: Cisco Systems, 2002, str. 9

Tokovna kriptografija predpostavlja uporabo mehanizma za generiranje toka bitov, ki jih z enostavnimi logičnimi operatorji (npr. ekskluzivni ali) združimo z berljivim sporočilom in dobimo šifrirano sporočilo. Pri takšnem šifriranju moramo biti pozorni na uporabo dovolj dolgih ključev (priporočljivo je njihovo navezovanje na predhodno šifrirano sporočilo).

3.3.2 Prednosti in slabosti simetričnih algoritmov

Sistem kriptografije, ki uporablja simetrični ključ, ima dve bistveni prednosti (Ramage, 2005):

a) je veliko hitrejši od asimetričnih sistemov,
b) zagotavlja zelo visoko stopnjo varnosti (ob uporabi dovolj dolgih ključev).

Slabosti simetrične kriptografije so (Wallhoff, 2002):

a) problem izmenjave ključev,
b) veliko število unikatnih ključev,
c) omejena varnost (omogoča zaupnost komunikacije, ne rešuje pa vprašanja pristnosti in nezanikanja),
d) večpasovna metoda (izmenjava ključev poteka po različnem kanalu kot izmenjava sporočila).

3.4 Asimetrična kriptografija (kriptografija javnega ključa)

Asimetrična kriptografija oziroma kriptografija javnega ključa se je razvila leta 1975 kot odgovor na dve pomembni vprašanji, na kateri simetrični algoritmi niso dali zadovoljivega odgovora. Prvo vprašanje oziroma problem je izmenjava ključev. Če želita dve osebi varno komunicirati, se morata vnaprej dogovoriti o uporabi enakega ključa. Nastopi problem izmenjave omenjenega ključa. Drugi problem, ki je povezan s prvim, je problem digitalnega podpisa. Določena oseba nam pošlje elektronsko sporočilo in pojavi se vprašanje, ali je prišlo sporočilo od te osebe ali morda od koga tretjega.

Problema sta na prvi pogled nerešljiva. Prvi problem izmenjave ključev pomeni, da morata osebi na varen način izmenjati ključa, toda ali ne bi raje v takšnem primeru izmenjala kar sporočilo? Drugi problem ni nič lažji. Podpis je enoznačen zgolj na papirju. Elektronski podpis je možno povsem brez težav prekopirati. Rešitev prinaša kriptografija javnega ključa, ki omogoča varno komunikacijo brez vnaprejšnjega dogovora o uporabi enakega ključa. Asimetrični algoritem sta leta 1976 uradno objavila Whitfield Diffie in Martin Hellman. Predstavila sta metodo varne izmenjave ključev, ki je postala znana kot Diffie-Hellmanova metoda. Navdih sta dobila pri Ralphu Merkleju, ki je tedaj proučeval distribucijo javnega ključa (Diffie, 1988).

Čeprav veljata Whitfield Diffie in Martin Hellman za očeta asimetrične kriptografije, njuna metoda rešuje zgolj vprašanje izmenjave tajnega ključa. Celovito rešitev asimetrične kriptografije, ki omogoča šifriranje, dešifriranje in digitalno podpisovanje sporočil, so leta 1978 prvič objavili Ron Rivest, Adi Shamir in Leonard Adleman. Algoritem se imenuje po inicialkah njihovih priimkov - RSA.

Zgodovina je nedavno postregla še z eno zanimivostjo. Leta 1997 so bili odprti dosjeji tajne službe angleške vlade GCHQ (Government Communications Headquarters), ki dokazujejo, da so znanstveniki James Ellis, Clifford Cocks in Malcolm Williamson odkrili postopek že v

začetku 70. let, kar je skoraj 30 let veljalo za skrbno varovano vojaško skrivnost (Cocks, 1973).

Ime asimetrična kriptografija nakazuje, da pri takšnem načinu ne uporabljamo istega ključa za šifriranje in dešifriranje (slika 3.9). Obstaja večje število asimetričnih algoritmov, ki uporabljajo različne metode in funkcije, vsem pa je skupna uporaba dveh ključev v paru, prvega (ključ 1) za šifriranje in drugega različnega (ključ 2) za dešifriranje. Ključa sta med seboj matematično povezana, vendar privatnega ključa ni možno izračunati iz javnega.

Slika 3.9: Asimetrično šifriranje

Vir: Jerman Blažič et al., 2001, str. 104

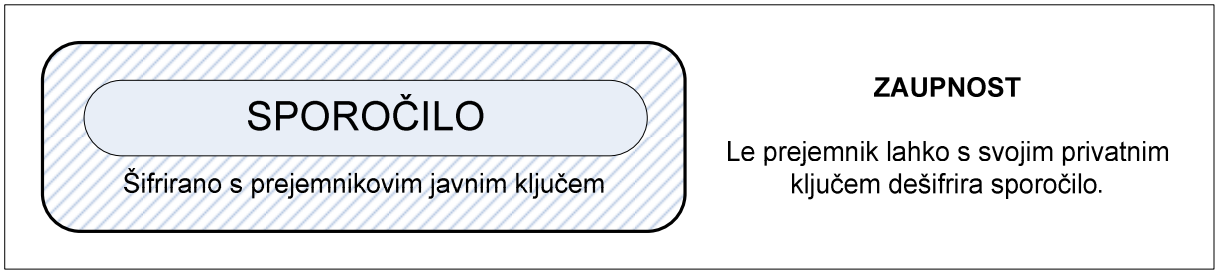
Ko želi Rok sporočilo varno poslati Katji, uporabi Katjin javni ključ 1 za šifriranje. Katja ima pri sebi skrbno varovan privatni ključ 2, ki lahko edini dešifrira sporočilo, šifrirano s ključem 1. Na prvi pogled se zdi, da javni ključ uporabljamo za šifriranje, privatnega pa za dešifriranje. Oba ključa lahko uporabljamo bodisi za šifriranje bodisi za dešifriranje. V primeru šifriranja z javnim ključem opravimo proces dešifriranja s privatnim in obratno. Torej ključa vedno nastopata v paru.

Katja lahko svoj javni ključ pošlje komurkoli, ki ji želi varno pošiljati pošto. Ključ je javen in ga lahko uporabljajo vsi potencialni pošiljatelji, za dešifriranje sporočila pa je možno uporabiti le njen privatni ključ. To pomeni, da za varno komunikacijo ne potrebujemo velikega števila unikatnih ključev, temveč zadošča en javno dostopen in en skrbno varovan privatni. Ugotovimo, da je omenjeni pristop veliko bolj priročen kot uporaba katere izmed tehnik simetrične kriptografije. Zaradi enostavnosti uporabe so javni ključi pogosto shranjeni v različnih javno dostopnih imenikih in bazah na internetu.

V poglavju o informacijski varnosti so navedene varnostne zahteve pri elektronskem poslovanju. Asimetrični kriptografski mehanizmi v različnih konfiguracijah zagotavljajo ***zaupnost***, ***pristnost*** in ***nezanikanje*** (Thorsteinson et al., 2003).

Rok želi poslati ***zaupno*** sporočilo Katji. Sporočilo bo šifriral s Katjinim javnim ključem in tako zagotovil zaupnost, le Katja lahko namreč s svojim privatnim ključem opravi proces dešifriranja (slika 3.10), drugim očem je sporočilo prikrito.

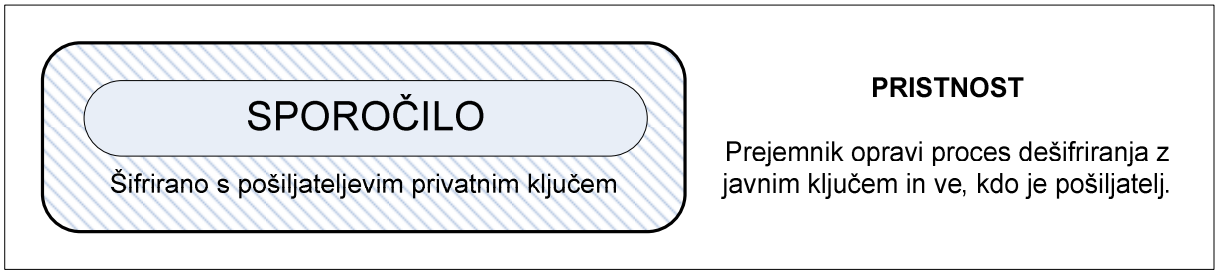
Slika 3.10: Zagotavljanje zaupnosti poslanega sporočila



Vir: Harris, 2003, str. 520

Če želi Rok poslati Katji ***pristno*** sporočilo, bo uporabil svoj privatni ključ. Za dešifriranje bo Katja uporabila Rokov javni ključ in se tako prepričala, da je on pošiljatelj sporočila (slika 3.11). Po drugi strani pa lahko takšno sporočilo dešifrirajo vsi, ki imajo dostop do Rokovega javnega ključa.

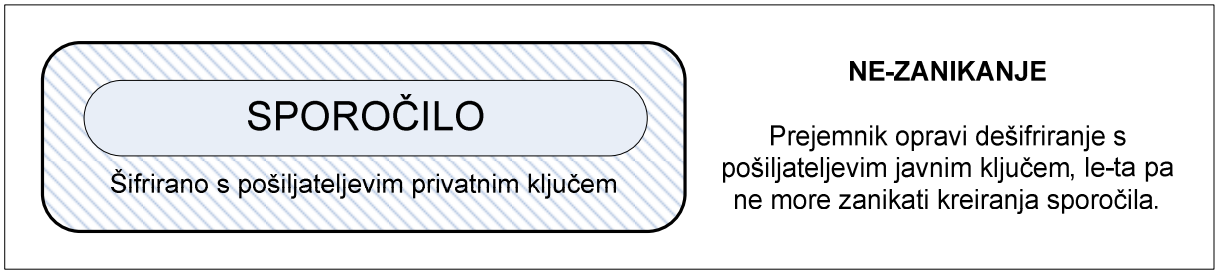
Slika 3.11: Zagotavljanje pristnosti poslanega sporočila



Vir: Harris, 2003, str. 520

Zgoraj omenjeni način uporabimo tudi za zagotavljanje ***nezanikanja***. Ko Katja z javnim ključem dešifrira Rokovo sporočilo, šifrirano z njegovim privatnim ključem, on ne more zanikati pošiljanja tega sporočila (slika 3.12).

Slika 3.12: Zagotavljanje nezanikanja poslanega sporočila

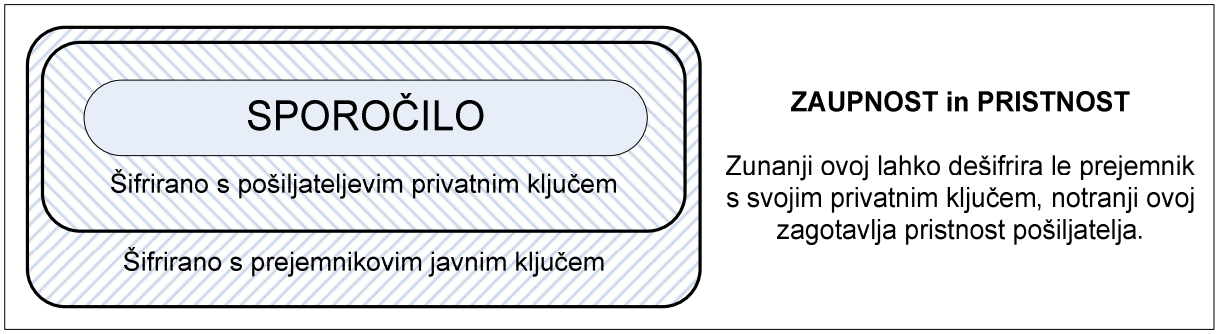


Vir: Harris, 2003, str. 520

Najbolj uporabna je kombinacija načinov, ki zagotavljata ***zaupnost*** in ***pristnost***. Rok najprej sporočilo šifrira s svojim privatnim ključem in nato še s Katjinim javnim ključem. Sporočilo lahko dešifrira le Katja in pride do sporočila, šifriranega z Rokovim privatnim ključem. Nato

uporabi Rokov javni ključ in se tako prepriča, da je on pošiljatelj (slika 3.13). S takšnim načinom zadostimo dvema bistvenima varnostnima zahtevama elektronskega poslovanja.

Slika 3.13: Zagotavljanje zaupnosti in pristnosti poslanega sporočila



Vir: Harris, 2003, str. 520

3.4.1 Prednosti in slabosti asimetričnih algoritmov

Prednosti in slabosti asimetričnih algoritmov presojamo v odnosu do simetričnih algoritmov. Pomembnejše prednosti so (Harris, 2003):

a) enostavnejša distribucija ključev,
b) večja prilagodljivost,
c) zagotavljanje varnostnih zahtev e-poslovanja (zaupnost, pristnost, nezanikanje).

Na asimetrične algoritme lahko pogledamo tudi z drugega zornega kota (Harris, 2003):

a) so veliko počasnejši od simetričnih,
b) zagotavljajo manjšo varnost kot simetrični.

3.5 Velikost ključa

Velikost ključa neposredno vpliva na varnost algoritma. V prejšnjih poglavjih smo videli, da je ponavadi algoritem splošno znan. Prav tako je relativno enostavno prestreči šifrirano sporočilo. Največja neznanka je torej poznavanje ključa. Ko najdemo ključ, je uganka rešena. Zato mora biti ključ skrbno izbran, njegove vrednost pa naj ne bi bilo mogoče uganiti. Pravimo, da mora biti nabor ključev čim večji (Ashley, 2005).

Velikost oziroma dolžino ključa merimo v bitih, ki so merilo za varnost sistema. Pri tem je pomembno ločiti med velikostjo ključa pri simetričnih in asimetričnih sistemih. Simetrični algoritmi temeljijo na relativno enostavni manipulaciji bitov. Ključi so na primer 40-bitni, 56-bitni, 128-bitni in tako naprej. Najbolj enostaven ključ bi imel 1 bit, kar pomeni vrednost 0 ali

1. Ključ z dvema bitoma omogoča vrednosti 00, 01, 10 in 11. Z vsakim bitom se podvoji število ključev. Simetričen algoritem DES uporablja 56-bitni ključ, kar pomeni, da je možnih 2^{56} oziroma 72.057.594.037.927.936 ključev. Odličen računalnik lahko preizkusi milijardo ključev na sekundo, kar pomeni, da bi potrebovali več kot 2 leti za preizkus vseh možnosti. Algoritem AES, ki je nadomestil DES, uporablja ključe z dolžino do 256 bitov. Na podlagi dosedanjih izkušenj takšnega števila kombinacij nikoli ne bo možno preizkusiti. Za simetrične algoritme pravimo, da zagotavljajo zadovoljivo raven varnosti pri velikosti ključa od 128 bitov naprej (Workman, 2005).

Asimetrični ključi se bistveno razlikujejo od simetričnih. Temeljijo na zahtevnosti matematičnih problemov, katerih reševanje je zelo dolgotrajno. Asimetričen algoritem RSA temelji na problemu faktorizacije dveh velikih praštevil. Medtem ko je množenje dveh velikih praštevil enostavno, je obraten postopek praktično nemogoč. Vzemimo na primer število 65. Kateri praštevili moramo zmnožiti, da dobimo omenjeni rezultat? Rešitev sta praštevili 5 in 13, do katerih pridemo s poskusi in napakami. Zaenkrat ni učinkovitega algoritma, ki bi lahko izračunal rezultat. Pri simetričnem algoritmu DES (56-bitni ključ) imamo 2^{56} možnih ključev. Ker imamo pri asimetričnih algoritmih opravka s praštevili, je možen nabor ključev manjši. Na odlični spletni strani o praštevilih »The Prime Pages« (http://primes.utm.edu/) uporabljajo formulo za približno ocenjevanje množice praštevil pod določenim številom x:

$$praštevila(ocena) = \frac{x}{\log(x) - 1} \tag{3.1}$$

Upoštevamo dolžino ključa $x = 2^{56}$ in izračunamo:

$$\frac{2^{56}}{\log(2^{56}) - 1} = 4.544.018.743.050.260 \; praštevil \; .$$

To pomeni, da je pri dolžini ključa 56 bitov nabor možnih ključev pri asimetrični kriptografiji za približno 16 krat manjši kot pri simetrični kriptografiji. Tabela 3.2 prikazuje primerljivo dolžino ključa pri zagotavljanju enake varnosti.

Tabela 3.2: Dolžina ključa pri približno enaki varnosti

Simetrični ključ (DES, 3DES, AES, IDEA…)	**Asimetrični ključ** (RSA, ELGAMAL, ECC)
56 bitov	384 bitov
64 bitov	512 bitov
80 bitov	768 bitov
112 bitov	1792 bitov
128 bitov	2304 bitov
192 bitov	7680 bitov
256 bitov	15360 bitov

Vir: Workman, 2005

Lahko si predstavljamo, da povprečni uporabnik ocenjuje kriptografske rešitve zgolj na podlagi dolžine ključa. Nič nenavadnega ni javni ključ velikosti 1024 bitov, ki na prvi pogled zagotavlja zadovoljivo varnost. Toda primerljiv simetričen ključ ima dolžino približno 90 bitov, kar ni pretirano veliko. Zaključimo, da je zaželena velikost simetričnega ključa 128 bitov, asimetričnega pa 2048 bitov.

4. KRIPTOGRAFSKI ALGORITMI V PRAKSI

4.1 Matematika v ozadju algoritmov

Namen poglavja ni poglobljena matematična razprava, temveč razlaga nekaterih osnovnih konceptov in temeljev, brez katerih ni možno razumevanje modernih kriptografskih algoritmov.

4.1.1 Ekskluzivni ali

Ekskluzivni ali (XOR) je ena izmed temeljnih matematičnih operacij kriptografskih algoritmov. Okoli leta 1850 je matematik George Boole razvil algebro, na kateri temeljijo mikroprocesorski računalniki. Definiral je primitivne logične operacije, ki imajo enega ali dva vhodna elementa in enega izhodnega. Boolove osnovne operacije so (Redshaw, 1996):

- NOT (negiranje): Izhodna vrednost je obratna od vhodne ali izhod je pravilen, če je vhod nepravilen, in obratno.
- AND (in): Izhod je pravilen, če so vsi vhodi pravilni, sicer je nepravilen.
- OR (ali): Izhod je pravilen, če je vsaj ena vhodna vrednost pravilna. Če sta obe vhodni vrednosti nepravilni, je izhod nepravilen.
- XOR (ekskluzivni ali): Izhod je pravilen, če je natančno en vhod pravilen in en nepravilen, sicer je napačen.

V nadaljevanju bomo predstavili logični operator ekskluzivni ali, ki ima dva vhoda in en izhod (tabela 4.1).

Tabela 4.1: Boolov operator (ekskluzivni ali)

Vhod 1	Vhod 2	Izhod (ekskluzivni ali)
0	0	**0**
0	1	**1**
1	0	**1**
1	1	**0**

Vir: http://www.learn-c.com/boolean.htm, 2005

Vsako sporočilo lahko drobimo do najmanjšega gradnika, ki ga imenujemo bit. Bit lahko zavzame vrednost 0 ali 1. Pri združevanju dveh bitov imamo 4 možne kombinacije in rezultat zavzame vrednost 0, če sta bita enaka oziroma vrednost 1, če sta bita različna. Za kriptografijo je ugotovitev zelo pomembna. Vzemimo sporočilo 1110001101 in ključ 1100100101 ter ju združimo z operatorjem ekskluzivni ali. Rezultat je zmešnjava bitov, ki so brez pomena.

sporočilo	1110001101
ključ	1100100101
ekskluzivni ali	0010101000

Originalno sporočilo izračunamo z obratnim postopkom. Z operatorjem ekskluzivni ali združimo bite ključa in rezultata ter dobimo izhodiščno sporočilo.

4.1.2 Modul

Zaradi omejene natančnosti računalnikov se pri računanju z velikimi realnimi števili soočamo z zaokroževanjem. Ker v kriptografiji približki ne zadoščajo, se poslužujemo končnih računskih obsegov. Takšni so praštevilski obsegi, v katerih računamo po modulu velikega praštevila. Enostavno povedano je modul funkcija ostanka. Razumevanje funkcije omogoča predstavitev enostavnih primerov:

1.) 9 mod 7 = 2 (ker je 9/7 = 1 in ostanek 2),
2.) 15 mod 7 = 1 (ker je 15/7 = 2 in ostanek 1),
3.) 25 mod 5 = 0 (ker je 25/5 = 5 in ostanek 0),
4.) 81 mod 17 = 13 (ker je 81/17 = 4 in ostanek 13).

Modul je v kriptografiji zelo uporaben, ker omogoča uporabo velikih števil in zagotavlja, da rezultat ne bo preveliko število, ki bi ga bilo potrebno zaokroževati.

4.1.3 Faktorizacija

Faktorizacija je razcepitev števila na manjša števila, ki pomnožena skupaj tvorijo izhodiščno število. Na primer faktorja števila 15 sta 3 in 5, ker pomnožena skupaj tvorita produkt 15. Problem faktoriranja je najti števili 3 in 5 ob danem številu 15.

Faktorizacija praštevil, ki jo uporabljamo pri kriptografiji, pomeni razcepitev števila na dve praštevili. Vsako celo število ima unikatni praštevili, ki pomnoženi skupaj tvorita omenjeno število. Postopek je za kriptografijo zanimiv, ker je dve veliki praštevili enostavno pomnožiti, medtem ko je faktorizacija zmnožka (obratni postopek) izjemno zahtevna in dolgotrajna.

4.1.4 Diskretni logaritem

Računanje potenc s celimi števili v zaprti množici je učinkovito, ne poznamo pa učinkovitega algoritma za obratni postopek, torej računanje diskretnega algoritma. Problem diskretnega algoritma se nanaša na poskus izračuna števila (Pistoia et al., 2004):

$$x = \log_g y \tag{4.1}$$

pri čemer je $y = g^x$ (g je znan, x pa je veliko število). Podobno kot pri problemu faktorizacije je rešitev diskretnega algoritma izredno zahtevna, kar predstavlja dober temelj za varnost kriptografskih algoritmov.

4.2 Simetrični kriptografski algoritmi

V nadaljevanju sledi predstavitev pomembnejših predstavnikov simetričnih kriptografskih algoritmov. Med seboj se razlikujejo po različnih metodah šifriranja in dešifriranja, vsem pa je skupna uporaba dveh enakih ključev.

4.2.1 DES

V 70. letih prejšnjega tisočletja se je pričelo obdobje rasti elektronske komunikacije znotraj ameriške vlade in privatnega podjetniškega sektorja. Po komunikacijskih medijih so se pretakale občutljive informacije, kot so na primer kapitalski transferi, vredni nekaj milijonov dolarjev, nakupi in prodaje vrednostnih papirjev, rezervacije letalskih letov, izmenjani podatki o zdravstvenem stanju pacientov itd. Z naraščanjem obsega in vrednosti informacij se pojavi zahteva po zaščiti pred morebitnimi zlorabami. Spomladi leta 1973 NBS (National Bureau of Standards) objavi javni razpis za pridobivanje predlogov kriptografskih algoritmov, ki bi zaščitili elektronske podatke (Ng et al., 2005).

Biro NBS je zaman čakal na odziv. Šele poleti 1974 je IBM predstavil svojo rešitev, ki je bila razvita pod imenom Lucifer. Biro je s pomočjo agencije za nacionalno varnost ocenil algoritem in ga leta 1977 z določenimi spremembami sprejel kot standard za zaščito podatkov DES (Data Encryption Standard). Obstajajo polemike, ki očitajo namerno oslabitev IBM-ove rešitve, s čimer naj bi si ameriška vlada zagotovila vpogled v elektronske komunikacije (Grabbe, 2005).

DES je bil vključen v večino pomembnejših komercialnih produktov in v skoraj vse vladne agencije, ki so zahtevale varno komunikacijo. Izkazal se je kot eden najmočnejših in najbolj

zanesljivih šifrirnih algoritmov. Na podlagi predloga instituta ANSI (American National Standards Institute) so leta 1980 algoritem DES sprejeli kot splošni bančni standard za varno elektronsko komunikacijo (Ng et al., 2005).

DES je bil dolgo zelo popularen in agencija za nacionalno varnost je bila prepričana, da je preveč javen in zato ogrožen. Objavili so, da od leta 1988 naprej ne bo v skladu s standardi in ga bo potrebno zamenjati. Kljub temu je bilo dokazano, da DES v praksi zagotavlja potrebno stopnjo varnosti, na trgu pa ni bilo primernega nadomestila. Zaradi polemik s stroko je agencija za nacionalno varnost ponovno pretehtala svojo odločitev in prižgala zeleno luč za petletno podaljšanje certifikata. Zmogljivost računalnikov je skokovito naraščala in leta 1998 je DES »padel« v pičlih treh dneh. Kot odgovor so ponudili 3DES, ki s šifriranjem, dešifriranjem in ponovnim šifriranjem sporočila z neodvisnimi ključi povečuje varnost (Schneier, 1998). Kljub temu je bil DES kasneje nadomeščen z algoritmom Rijndael kot AES (Advanced Encryption Standard), ki je bil sprejet kot nova metoda šifriranja občutljivih vladnih informacij. Pričakovati je, da bo široko sprejet tudi v privatnem sektorju.

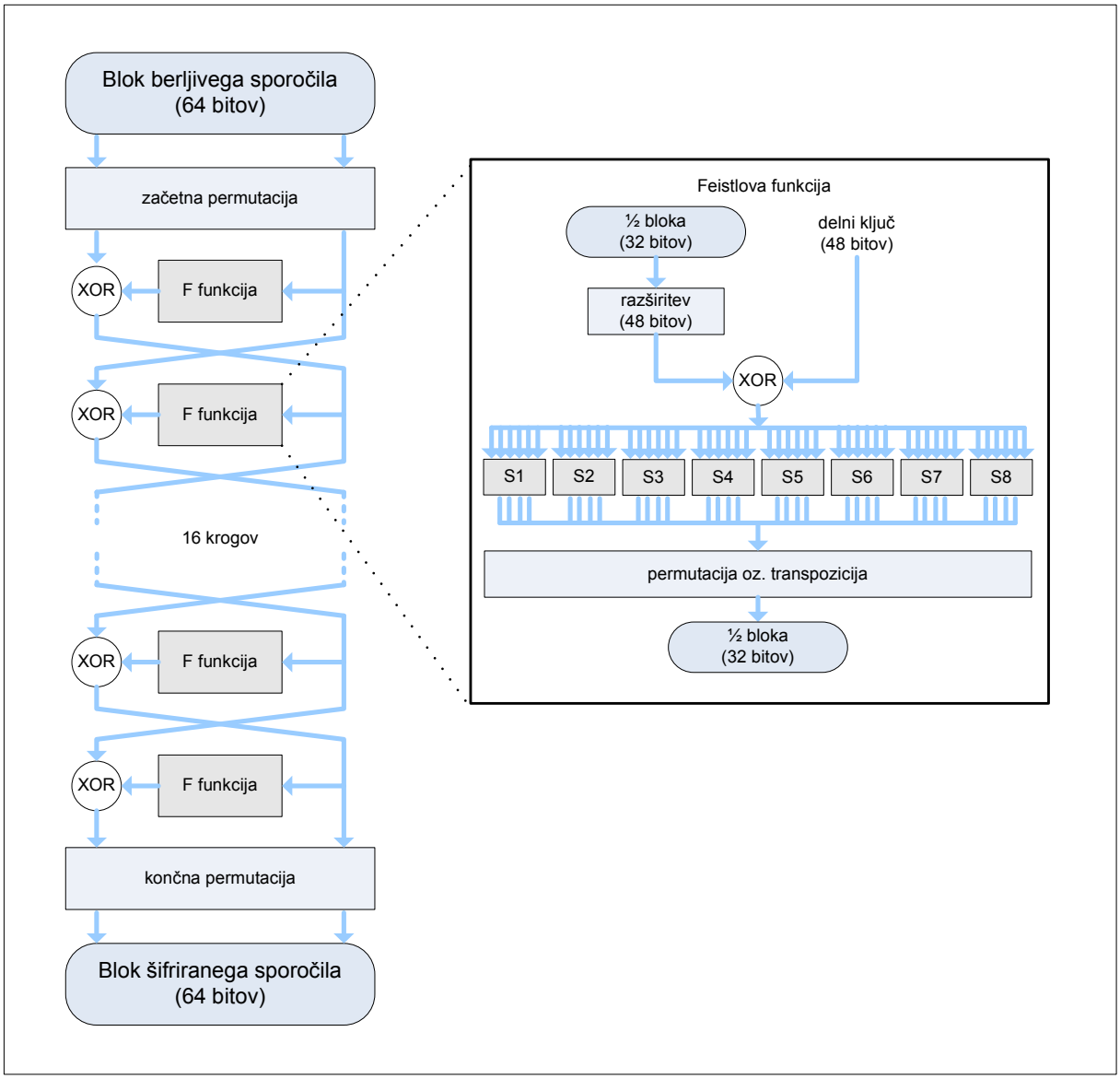
DES uvrščamo med blokovne algoritme, ki berljivo sporočilo najprej razdeli na 64-bitne bloke ter kasneje v procesu na 32-bitne bloke. Vsak blok gre skozi 16 krogov zahtevnih transpozicij in substitucij, katerih rezultat je odvisen od vrednosti ključa. S tem se zagotavlja zmešnjava in razpršitev, kar je pogoj za varen mehanizem. DES je simetričen algoritem, ki uporablja enak ključ za šifriranje in dešifriranje. Velikost glavnega ključa je 64 bitov, dejansko tvori ključ 56 bitov, preostalih 8 bitov se uporablja za pariteto. Glavni ključ je razdeljen na 16 unikatnih delnih ključev, od katerih je vsak namenjen svojemu krogu. Rezultat algoritma je 64-bitni blok šifriranega sporočila (Coppersmith, 1994).

Struktura algoritma DES je prikazana na sliki 4.1. Proces je sestavljen iz 16 enakih korakov in vsebuje začetno ter končno permutacijo, ki sta zrcalni. Omenjeni permutaciji sta vključeni zaradi lažjega razporejanja blokov pri relativno šibki procesorski moči računalnikov v 70. letih in nimata večjega kriptografskega pomena. Proces blok razpolovi na dve polovici po 32 bitov, ki sta obravnavani izmenično. Takšna shema je znana kot Feistlova shema, ki zagotavlja podobnost procesa šifriranja in dešifriranja. Razlika med procesoma je v uporabljenem vrstnem redu ključev. Za dešifriranje uporabimo obratni vrsti red kot pri šifriranju. Algoritem se pri tem ne spreminja, kar zelo poenostavlja implementacijo v praksi (Fischer, 2005).

Feistlova funkcija (F-funkcija) blok 32 bitov s podvajanjem določenih bitov razširi na 48 bitov ter jih s pomočjo ekskluzivnega ali združi z delnim ključem. Glavni ključ, ki ga uporabljamo pri šifriranju in dešifriranju, je razdeljen na 16 delnih ključev in vsak korak procesa uporabi unikaten delni ključ. Nadalje pridobljenih 48 bitov razdelimo na osem 6-bitnih enot, ki jih s pomočjo nelinearne substitucije prevedemo v osem 4-bitnih enot. To je osrednji del DES-a, ki

zagotavlja varnost. Dobljenih 32 bitov s pomočjo permutacij prevedemo v 32 bitov, ki vstopijo v novi krog in tako dalje (sika 4.1).

Slika 4.1: Algoritem DES



Vir: http://www.mathdaily.com/lessons/DES, 2005

DES ima 4 različne oblike, ki se uporabljajo v različnih okoliščinah z različnimi nameni. Določena oblika lahko veliko bolje deluje v specifičnem okolju kot druga oblika. Zato je potrebno oblike dobro poznati in jih implementirati v skladu s situacijo in namenom (Schneier, 1996):

1. ECB (Electronic Code Book Mode) je privzeta DES-ova oblika in deluje kot knjiga šifer. V algoritem s ključem vstavimo blok 64 bitov in rezultat je šifriranih 64 bitov. Enako

nešifrirano sporočilo in enak ključ vedno generirata enako šifrirano sporočilo. Vsak ključ ima različno šifrirno knjigo, ki vsebuje navodila za izvedbo substitucij in permutacij. Omenjena oblika se uporablja za manjše količine podatkov, ker je šifriranje bloka neodvisno od drugih blokov. Oblika je zelo uporabna pri podatkovnih bazah, kjer se naključno dostopa do različnih podatkov. Omogočeno je dodajanje, brisanje, šifriranje in dešifriranje posameznega zapisa ali tabele neodvisno od ostalih zapisov. Druge oblike DES-a so odvisne od teksta pred njimi, kar otežuje šifriranje in dešifriranje manjših količin podatkov. Primer implementacije v praksi je zaščita PIN-številke na bančnih avtomatih.

2. CBC (Cipher Block Chaining Mode) ne odkrije morebitnega vzorca kot v prejšnji obliki ECB, ker je poleg podatkovnega bloka in ključa v algoritem vključena vrednost predhodnega podatkovnega bloka, kar zagotavlja naključni šifriran tekst. Rezultat prvega bloka vpliva na drugega in tako naprej, kar vodi v verižni učinek. Specifični blok je odvisen od vseh predhodnih blokov in postopek nima vzorca.

3. CFB (Cipher Feedback Mode) je zelo podobna obliki CBC, vendar namesto vrednosti predhodnega podatkovnega bloka uporablja šifrirano vrednost predhodnega bloka. Primerna je za šifriranje posameznih znakov, kar je sicer domena tokovne kriptografije.

4. OFB (Output Feedback Mode) spominja na tipično tokovno kriptografijo, ker oblikuje tok naključnih bitov, s katerimi šifrira sporočilo. Nato šifrirano sporočilo uporabi kot generator novega toka bitov za naslednje sporočilo.

Sklepamo lahko, da je bil algoritem DES relativno varen v preteklosti, ko računalniki niso bili dovolj zmogljivi. Najpogostejša in najbolj enostavna metoda napada je t. i. surovi napad, ko napadalec preizkuša ustreznost vsakega ključa posebej. Dolžina ključa določa število vseh možnih ključev in posledično smiselnost takšnega napada. Algoritem DES uporablja 56-bitni ključ, kar je relativno malo. Ni skrivnost, da je IBM predvidel uporabo 128-bitnega ključa, vendar je pod pritiski agencije za nacionalno varnost pristal na uporabo 64-bitnega oziroma 56-bitnega ključa, če odštejemo 8-bitov za pariteto. Sklepamo lahko, da je imela omenjena agencija že v 70. letih prejšnjega tisočletja dovolj zmogljive računalnike za razbitje 56-bitnega ključa. Že leta 1977 sta Diffie in Hellman predlagala izgradnjo računalnika, za katerega bi potrebovali približno 20 mio USD in bi našel DES-ov ključ v enem dnevu. Podobno idejo je imel leta 1993 Michael Wiener, ki je predlagal izgradnjo računalnika za 1 mio USD. Pravi ključ naj bi našel v 7 urah. Poizkusi so bolj ali manj ostali v teoretičnih okvirih in na papirju. Leta 1997 pa je podjetje RSA Security sponzoriralo tekmovanje z glavno nagrado v višini 10.000 USD za prvega posameznika ali skupino, ki bi razbila šifro. Zmagal je projekt DESCHALL (DES Challenge), ki so ga vodili Rocke Verser, Matt Curtin in Justin Dolske. Uporabili so moč nekaj tisoč računalnikov, priključenih na internet in DES je bil »razbit«.

Leto kasneje organizacija EFF (Electronic Frontier Foundation) za približno 250.000 USD zgradi računalnik, imenovan »DES cracker«, ki je našel pravi ključ po dveh dneh iskanja. Očitno je razvoj računalnikov prehitel DES in njegova varnost ni več zadovoljiva (EFF, 2005).

4.2.2 3DES

Z razvojem računalnikov je postal algoritem DES ranljiv. Leta 1999 Institut za standarde in tehnologijo priporoči uporabo 3DES (Triple DES), ki temelji na DES-u. Avtor omenjenega algoritma je Walter Tuchman, ki je vodil razvoj DES-a na IBM v 70. letih. 3DES uporablja enak algoritem kot DES, le da se proces ponovi trikrat (slika 4.2).

Možni sta dve osnovni metodi: DES-EEE in DES-EDE. Prva v vseh treh korakih uporablja šifriranje, medtem kot druga predvideva uporabo šifriranja, nato dešifriranja in ponovno šifriranja s tremi različnimi neodvisnimi ključi. Postopek dešifriranja poteka v obratnem vrstnem redu. Najprej dešifriramo s ključem 3, nato šifriramo s ključem 2 in dešifriramo s ključem 1.

3DES uporablja 168-bitni ključ (trije neodvisni ključi po 56 bitov) in 48 krogov izračunov, kar pomeni, da je približno 2^{56} krat močnejši od DES-a. Zaradi zahtevnega procesa je tudi nekajkrat počasnejši.

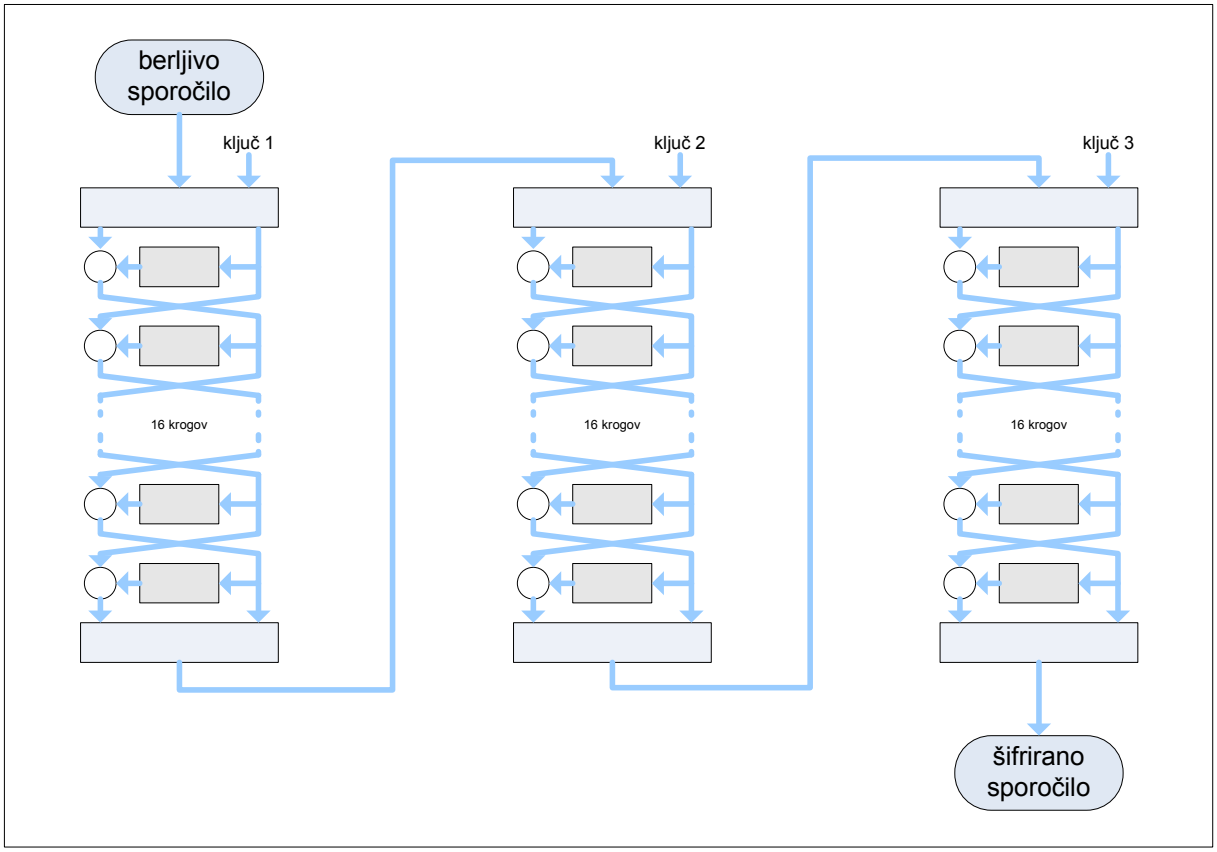
Prednosti 3DES-a so predvsem (Castelino, 2005):

- enostavna implementacija v praksi,
- temelji na DES-u, ki je bil v uporabi 25 let in je preizkušen,
- velika hitrost v primerjavi z asimetričnimi algoritmi.

Slabosti predstavljajo relativno nizka hitrost glede na novejše simetrične algoritme, problem izmenjave ključa in naklonjenost novim standardom.

Pri trenutni moči računalnikov lahko 3DES zagotavlja sprejemljivo raven varnosti. Kljub temu se v praksi pojavljajo novejši algoritmi, kot je AES s privzetim algoritmom Rijndael, ki se je kot zelo hiter izkazal tako pri programskih kot strojnih izvedbah. Poleg tega je njegova implementacija v praksi nezahtevna (Castelino, 2005).

Slika 4.2: Struktura algoritma 3DES



Vir: http://upload.wikimedia.org/wikipedia/commons/b/b7/3des-overall-view.png, 2005

4.2.3 AES

DES je bil kot kriptografski standard v uporabi preko 25 let. Mnogi strokovnjaki so se strinjali, da je potrebno razviti nov standard, ki bi odražal zahteve in tehnologijo tega časa. Največji očitek DES-u je 56-bitni ključ, ki ne zagotavlja zadovoljive varnosti. Poleg tega je bil oblikovan predvsem za uporabo v strojni opremi, kjer je dosegal zadovoljive hitrosti. Nasprotno je bil proces pri programskih rešitvah izjemno počasen. 3DES je rešil problem velikosti ključa in njegove varnosti, vendar je v programskih rešitvah še počasnejši od DES-a. Posledično je Inštitut za standarde in tehnologijo (NIST) objavil javni razpis zbiranja predlogov naprednega kriptografskega standarda. Inštitut je zahteval simetrični blokovni algoritem s podporo za 128-, 192- in 256-bitne ključe. V ožji izbor je prišlo 5 algoritmov (Srinivas, 2000):

- MARS (IBM Team),
- RC6 (RSA Laboratories),
- SERPENT (Ross Anderson, Eli Biham, Lars Knudsen),
- TWOFISH (Counterpane Systems),
- RIJNDAEL (Joan Daemen, Vincent Rijmen).

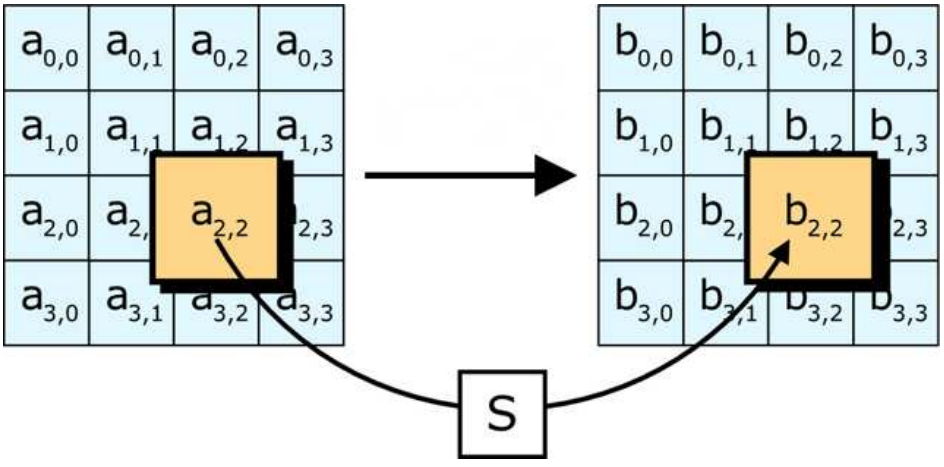
Izbor se je začel septembra 1997 in je trajal 3 leta. Postopek je bil razdeljen na nekaj krogov, ki so se zaključevali z javnimi delavnicami in razpravami. Vsak algoritem je bil ocenjen z vidika varnosti, stroškov, lastnosti in izvedbe v praksi. Oktobra 2000 je NIST objavil, da je bil kot bodoči standard AES (Advanced Encryption Standard) izbran algoritem Rijndael, ki sta ga razvila belgijska kriptografa Joan Daemen in Vincent Rijmen. Glavne lastnosti izbranega algoritma so odpornost proti vsem znanim napadom, enostaven model in strnjena koda, ki omogoča hitrost na raznolikih platformah (Brown, 2002).

Če smo povsem natančni, AES ni absolutni sinonim za Rijndael. Algoritem Rijndael omogoča velikost blokov med 128 bitov in 256 bitov, medtem ko standard AES predvideva zgolj uporabo enotne 128-bitne velikosti bloka. Nadalje algoritem Rijndael omogoča različne velikosti ključev: 128-, 160-, 192-, 224- in 256-bitne. AES dovoljuje zgolj uporabo 128-, 192- in 256-bitnih ključev (Daemen et al., 2002).

Z algoritmom Rijndael se konča doba Feistlove funkcije oziroma mreže, ki je temelj mnogih simetričnih algoritmov. Rešitev je hitra tako pri programskih kot strojnih izvedbah, je relativno enostavna za implementacijo v praksi in ne potrebuje veliko spomina. Rijndael pri procesu šifriranja uporablja tabelo 4 x 4, kjer vsako polje zavzame bajt oziroma 8 bitov. Skupaj tabela vsebuje 16 bajtov oziroma 128 bitov, kar ustreza velikosti bloka. Število krogov je odvisno od velikosti ključa. Pri velikosti ključa 128 bitov se algoritem izvaja v 10 krogih, pri velikosti 192 bitov v 12 krogih in velikosti 256 bitov v 14 krogih. Vsak krog procesa razen zadnjega je sestavljen iz 4 korakov (Daemen et al., 2002):

1.) Nelinearna substitucija, kjer vsak bajt neodvisno vstopi v S-škatlo, ki ga transformira v novo vrednost. Operacija zagotavlja nelinearnost šifre (slika 4.3).

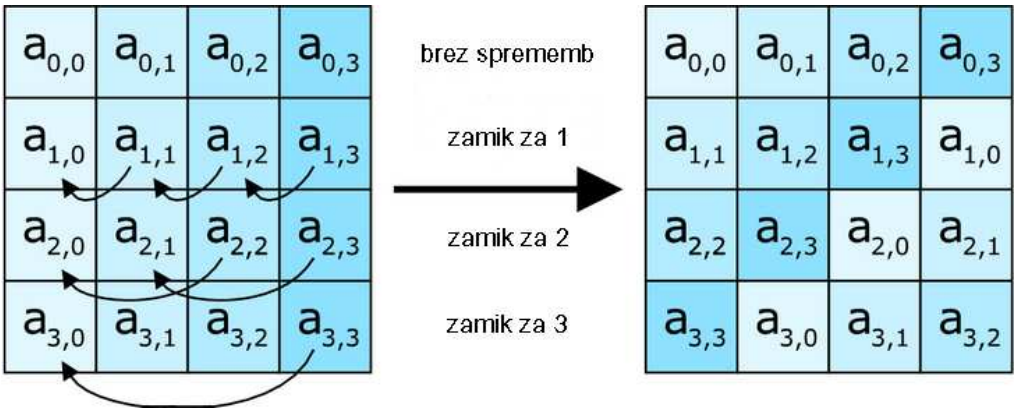
Slika 4.3: Rijndael, prvi korak (substitucija)



Vir: http://en.wikipedia.org/wiki/Image:AES-SubBytes.png, 2005

2.) Transpozicija, ki bajte znotraj vrstice ciklično zamika z določenim korakom. Prva vrstica ostane nespremenjena, druga je zamaknjena za eno mesto v levo, tretja za dve mesti in četrta za tri mesta (slika 4.4). Tako dosežemo, da ima vsak novi stolpec bajte vseh štirih prejšnjih stolpcev.

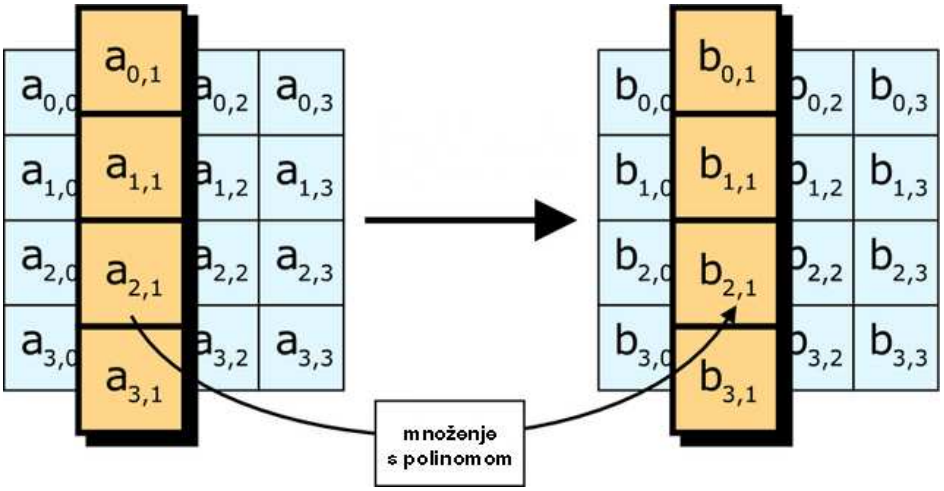
Slika 4.4: Rijndael, drugi korak (transpozicija)



Vir: http://en.wikipedia.org/wiki/Image:AES-ShiftRows.png, 2005

3.) Mešanje stolpcev, pri čemer vzamemo posamezen stolpec bajtov in ga matrično pomnožimo s fiksnim polinomom $c(x) = 3 \cdot x^3 + x^2 + x + 2$. Enako naredimo z drugimi stolpci (slika 4.5). Združena koraka 2 (transpozicija) in 3 (mešanje stolpcev) zagotavljata razpršitev šifre.

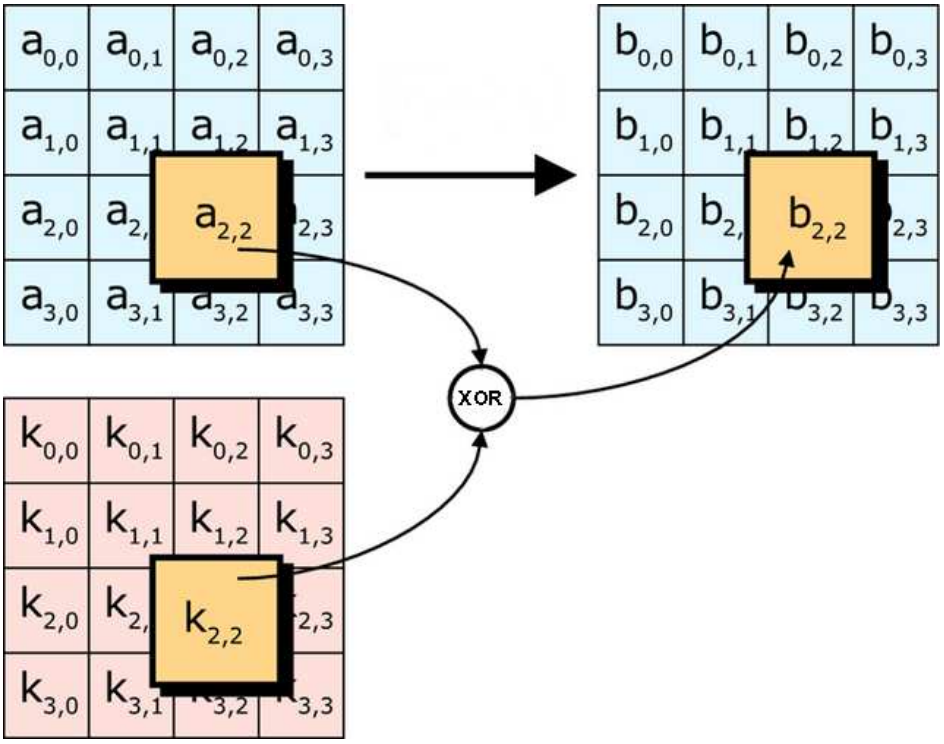
Slika 4.5: Rijndael, tretji korak (množenje s polinomom)



Vir: http://en.wikipedia.org/wiki/Image:AES-MixColumns.png, 2005

4.) V zadnjem koraku združimo (ekskluzivni ali) posamezni bajt z določenim delom ključa. Delni ključi tvorijo tabelo 4 x 4, ki je enake velikosti kot izhodiščni blok (slika 4.6).

Slika 4.6: Rijndael, četrti korak (ekskluzivni ali z delnim ključem)



Vir: http://en.wikipedia.org/wiki/Image:AES-AddRoundKey.png, 2005

Število krogov je odvisno od velikosti ključa in se ponavljajo z izjemo zadnjega kroga, ki ne vključuje tretjega koraka, mešanja stolpcev oziroma množenja s polinomom.

Način delovanja in zadovoljiva dolžina ključev standarda AES zadoščata za zaščito najbolj občutljivih vladnih informacij. V primeru zaščite tajnih dokumentov je priporočljiva uporaba 192- ali 256-bitnih ključev. Do zaključka tega dela ni bilo znanih omembe vrednih vdorov oziroma uspešnih napadov na omenjeni algoritem.

4.2.4 IDEA

Algoritem IDEA (International Data Encryption Algorithm) sta v zgodnjih devetdesetih razvila Xuejia Lai in James L. Massey kot rezultat skupnega projekta ETH (Swiss Federal Institute of Technology) in podjetja Ascom-Tech AG iz Švice. Cilj projekta je bil razvoj močnega šifrirnega algoritma, ki bi nadomestil DES (Lai et al., 1992).

Algoritem je patentno zaščiten, vendar je omogočena brezplačna uporaba za nekomercialne namene. Algoritem je izredno močan in velja za enega bolj zanesljivih. Vključen je tako v programske kot strojne rešitve.

IDEA uporablja 64-bitne bloke in 128-bitni ključ. Blok sporočila gre skozi osem enakih krogov in uporablja tri različne matematične operacije, ki so algebraično nekompatibilne. To so modularno seštevanje, množenje in ekskluzivni ali. IDEA je blokovni algoritem in ga je, tako kot DES, možno uporabljati v 4 različnih oblikah: ECB, CBC, CFB, OFB (Arild, 1998).

Ko je Phil Zimmermann razvijal rešitev PGP za zaščito elektronske pošte in datotek, je iskal najbolj varen algoritem. Rešitev je našel v algoritmu IDEA, ki ponuja zanesljivo strukturo in dober ugled. Na trgu obstaja večje število raznovrstnih varnostnih aplikacij, ki uporabljajo omenjeni algoritem. Razvoj je šel naprej in nosilec licence, švicarsko podjetje MediaCrypt, maja 2005 predstavi naslednika IDEA NXT, ki prav tako uporablja robustno Lai-Massey shemo (MediaCrypt, 2005).

4.2.5 BLOWFISH

Blowfish je simetričen algoritem s 64-bitnimi bloki, ki ga je leta 1993 razvil Bruce Schneier kot nadomestilo za DES. Rešitev je vgrajena v večje število aplikacij in algoritem do danes ne beleži pomembnejših vdorov.

Uporablja variabilno dolžino ključa, od 32 bitov pa vse do 448 bitov. Skozi čas je bil temeljito testiran in postopoma pridobiva sloves močnega in zanesljivega algoritma. Blowfish uporablja Feistlovo mrežo, bloki podatkov pa potujejo skozi 16 krogov različnih matematičnih funkcij, in to veliko hitreje kot pri algoritmu DES ali IDEA. Avtor je brezplačno objavil izvorno kodo in ne zahteva licenc, kar omogoča popolnoma prosto uporabo (Schneier, 1994).

Zadnje čase je pozornost usmerjena v novejše algoritme, ki podpirajo večjo velikost blokov. Takšen primer je Twofish, ki uporablja 128-bitne bloke in variabilni ključ do velikosti 256 bitov. Avtorji algoritma so izjemni kriptografski strokovnjaki Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall in Niels Ferguson. Omenjeni algoritem je bil eden izmed petih finalistov tekmovanja za AES, kjer je bil izbran Rijndael. Do danes ni znanih uspešnih napadov, njegova uporaba pa je popolnoma brezplačna in prosta, kot pri njegovem predhodniku Blowfishu (Schneier, 2005).

4.2.6 RC5

Algoritem RC5 (Rivest Cipher 5) je leta 1994 razvil kriptografski guru Ron Rivest iz MIT-a. Vse od objave naprej je zaradi svoje enostavnosti pritegnil pozornost mnogih raziskovalcev kriptografije, ki so skušali analizirati njegovo zanesljivost in varnost.

Algoritem je nastavljiv z različnimi parametri. Prvi parameter je podatkovni blok, ki lahko zavzema vrednosti 32, 64 ali 128 bitov. Sledi parameter krogov, ki omogoča razpon od 0 do 255 in so odvisni od podatkov, ki jih šifriramo. Zadnji parameter je ključ in njegova velikost zavzema od 0 do 2048 bitov. Privzeta vrednost je 64-bitni blok, 128-bitni ključ in 12 krogov. Omenjena variabilnost omogoča fleksibilnost na vseh ravneh varnosti. Jedro algoritma predstavlja Feistlova mreža, ki je enaka kot pri DES-u. Zasnova omogoča enostavno implementacijo v praksi, rešitev pa je analiziralo podjetje RSA Data Security, ki je algoritem leta 1997 tudi patentiralo (Rivest, 1997).

Kasneje je skupina kriptografov z Ronom Rivestom na čelu razvila algoritem RC6, ki temelji na RC5 in je bil eden izmed petih finalistov tekmovanja za AES. Poenostavljeno lahko rečemo, da je RC6 enak prepletanju dveh vzporednih RC5 procesov.

4.3 Asimetrični kriptografski algoritmi

V nadaljevanju sledi predstavitev pomembnejših predstavnikov asimetričnih kriptografskih algoritmov. Med seboj se razlikujejo po različnih metodah šifriranja in dešifriranja, vsem pa je skupna uporaba dveh različnih ključev, javnega in privatnega.

V prejšnjih poglavjih smo opisovali simetrične algoritme, ki na vsaki strani procesa uporabljajo enak ključ. Nismo si posebej zastavljali vprašanja, kako stranki varno izmenjata ključ (npr. fizično, z disketo v roki). Takšen način ni vedno priročen in v tem poglavju predstavljamo asimetrične algoritme, ki ponujajo odgovor na zastavljeno dilemo.

4.3.1 Diffie-Hellmanova izmenjava ključa

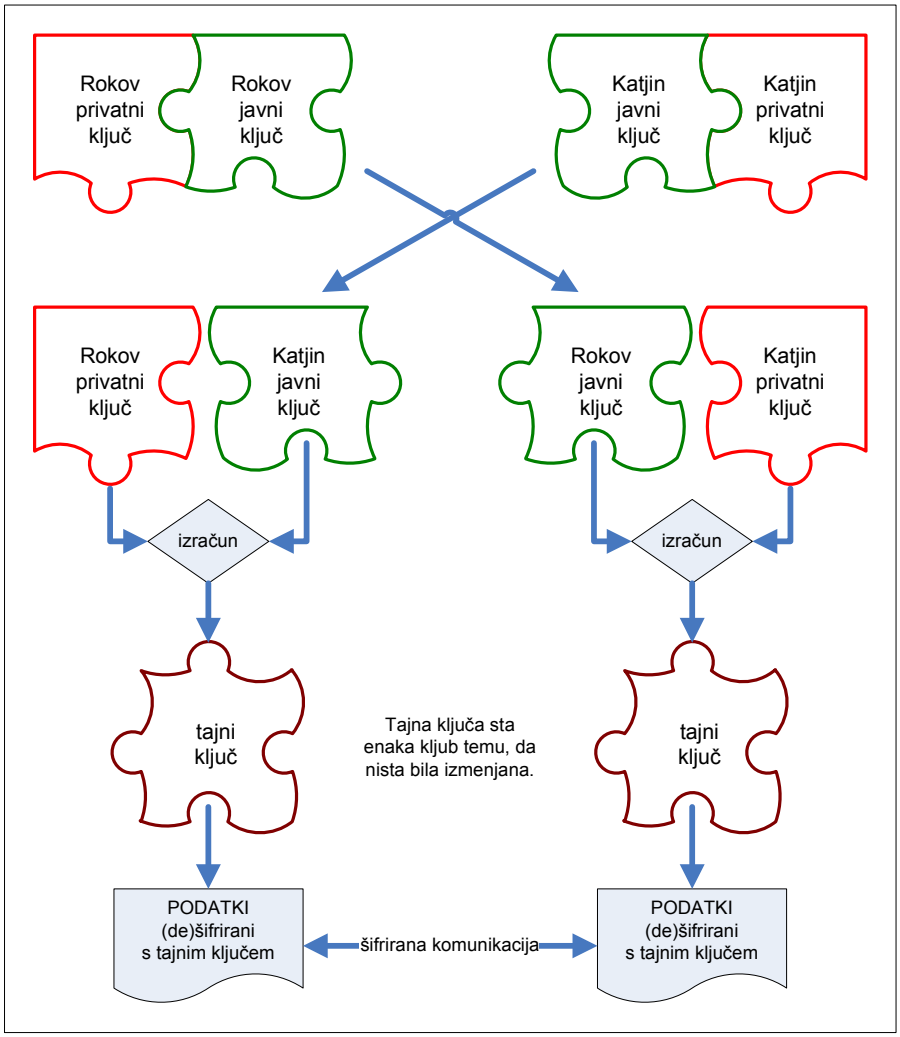
Diffie-Hellmanov algoritem za izmenjavo ključev je protokol, ki omogoča posameznikoma, da preko komunikacijskega kanala varno izmenjata tajni ključ, ne da bi predhodno izmenjala ključ za varno komunikacijo. Rešitev, ki temelji na delu Ralfa Merkleja, sta Whitfield Diffie in Martin Hellman prvič objavila leta 1976 (Diffie, 1988).

Algoritem rešuje zgolj problem izmenjave ključa in se ne ukvarja s samim šifriranjem in dešifriranjem sporočil. Po izmenjavi tajnega ključa se stranki dogovorita o uporabi ene izmed simetričnih tehnik kriptografije. Temelj algoritma predstavlja matematični trik, ki omogoča

enostavno računanje eksponentov, medtem kot je obraten postopek, izračun diskretnega algoritma, praktično nemogoč (Rescorla, 1999).

Slika 4.7 poenostavljeno prikazuje Diffie-Hellmanovo izmenjavo ključa. Posameznika (Rok in Katja), ki želita varno komunicirati, najprej izračunata vsak svoj privatni ključ in nato javni ključ. Vsak zase skrbno varujeta privatni ključ, javna ključa izmenjata. Pri tem je pomembna ugotovitev, da sta privatni in javni ključ matematično povezana. Javni ključ izračunamo iz privatnega, medtem ko varnost algoritma temelji na spoznanju, da je privatni ključ nemogoče izračunati iz javnega. Nadalje s pomočjo Diffie-Hellmanovega algoritma na podlagi svojega privatnega in tujega javnega ključa izračunata tajni ključ, ki je identičen in ga lahko uporabljata za šifriranje podatkov z različnimi simetričnimi algoritmi (Palmgren, 2005).

Slika 4.7: Diffie-Hellmanova izmenjava ključa



Vir: Palmgren, 2005, str. 5

Sledi matematični opis algoritma. Rok in Katja se želita dogovoriti o uporabi skupnega ključa za šifriranje njune komunikacije. V prvem koraku se dogovorita o uporabi dveh skrbno izbranih velikih praštevil g in p, ki ju javno izmenjata. Rok izbere naključno število x in izračuna (McSweeney, 2005):

$$rk = g^x \bmod p \tag{4.2}$$

Katja neodvisno izbere število y in izračuna:

$$ktj = g^y \bmod p \tag{4.3}$$

Izračunana rezultata rk in ktj medsebojno izmenjata ter izračunata vsak svoj ključ:

$$ključ_{Rok} = ktj^x \bmod p \tag{4.4}$$

$$ključ_{Katja} = rk^y \bmod p \tag{4.5}$$

$$ključ_{Rok} = ključ_{Katja}$$

Tako Rok in Katja dobita enaka ključa, ki ju lahko uporabita za šifriranje njune komunikacije. V ozadju algoritma je matematična teorija, ki omogoča enosmerno računanje:

$$ključ_{Rok} = ktj^x \bmod p \text{ in } ktj = g^y \bmod p \text{ sledi } ključ_{Rok} = (g^y \bmod p)^x \bmod p = g^{yx} \bmod p$$

$$ključ_{Katja} = rk^y \bmod p \text{ in } rk = g^x \bmod p \text{ sledi } ključ_{Katja} = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$$

Zaključimo, da sta ključa enaka:

$$g^{yx} \bmod p = g^{xy} \bmod p = ključ_{Rok} = ključ_{Katja}$$

Primer izračuna. Rok in Katja se dogovorita za uporabo števila $g = 24$ in števila $p = 13$. Recimo, da Rok neodvisno v svojih izračunih uporabi število $x = 5$, Katja pa število $y = 2$.

$$rk = g^x \bmod p = 24^5 \bmod 13 = 7$$
$$ktj = g^y \bmod p = 24^2 \bmod 13 = 4$$

Rok je izračunal število 7, Katja pa število 4. Izmenjata števili in izračunata vsak svoj ključ.

$$ključ_{Rok} = ktj^{x} \bmod p = 4^{5} \bmod 13 = 10$$
$$ključ_{Katja} = rk^{y} \bmod p = 7^{2} \bmod 13 = 10$$

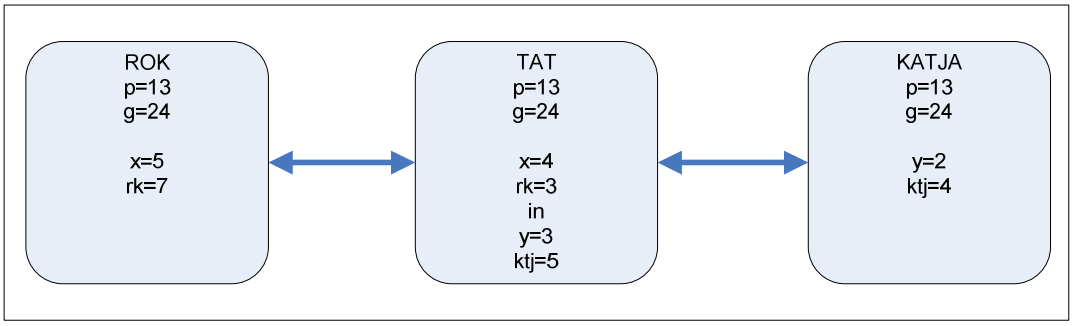
Pokazali smo, kako Rok in Katja z izračunom prideta do istega števila oziroma tajnega ključa. Dejansko izmenjata le 4 števila. Skupaj se dogovorita za števili g in p ter izmenjata števili rk in ktj, ki sta izračunani na podlagi skrbno varovanih števil x in y. Prikazani izračun namenoma uporablja majhna števila zaradi nazornosti in očitno je, da varnost s tem ni zagotovljena. Ob predpostavki uporabe velikih števil (100 mestna števila in več), pa je praktično nemogoče izračunati x in y ter posledično ključ.

Problem algoritma

Sklepali bi lahko, da Diffie-Hellmanova izmenjava ključa rešuje problem varnosti. Vendar se protokol izkaže za neučinkovitega v primeru napada »posrednika« (Man-In-The-Middle Attack). Posrednik prestreže vso komunikacijo med partnerjema in z obema deli tajni ključ (Aniket et al., 2004).

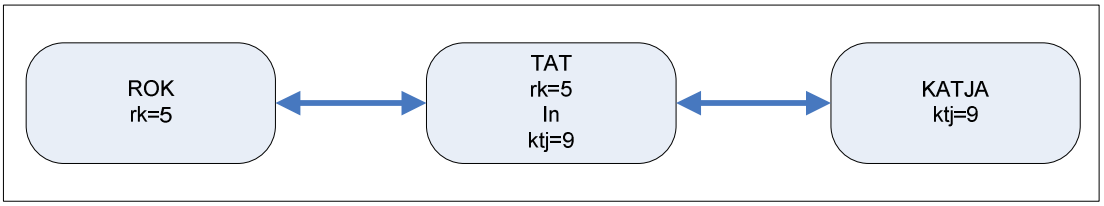
Zgodbo nadaljujemo iz zgoraj predstavljene komunikacije med Rokom in Katjo. Dodamo še tretjo osebo, ki jo bomo imenovali Tat. Nepridiprav prisluškuje komunikaciji med Rokom in Katjo ter prestreže števili $g = 24$ in $p = 13$. Igra vlogo posrednika, ki je Roku in Katji neznan (slika 4.8). Rok in Katja vsak zase izbereta naključno število. Rok izbere $x = 5$, Katja pa $y = 2$ (enako kot v prejšnjem primeru). Nepridiprav naključno izbere dve svoji števili, $x = 4$ in $y = 5$. Na podlagi znanega Diffie-Hellmanovega algoritma vsak zase izračunajo pripadajoče rk in ktj. Rok pošlje $rk = 7$ Katji. Tat prestreže število in namesto $rk = 7$ pošlje Katji lastno izračunani $rk = 3$. Katja neodvisno pošlje $ktj = 4$ Roku, vendar Tat informacijo prestreže in pošlje Roku $ktj = 5$.

Slika 4.8: Napad posrednika



Na podlagi izmenjanih števil izračunajo ključe. Na sliki 4.9 vidimo, da lahko Tat komunicira tako z Rokom kot Katjo, medtem ko onadva med seboj ne moreta, česar ne vesta, Tat namreč prestreže Rokovo sporočilo, ga prekopira oziroma priredi in zašifrira s Katjinim ključem ter ga posreduje naprej. Katja verjame, da je sporočilo prejela od Roka, vendar je pravi pošiljatelj Tat.

Slika 4.9: Tajni ključi v primeru napada posrednika



Ugotovitev je boleča, ker sta Rok in Katja prepričana, da komunicirata med seboj, vendar vsak zase ločeno komunicirata s Tatom. Ugotovitvi navkljub ni vse izgubljeno, rešitev se namreč skriva v digitalnem podpisu, ki enoznačno identificira pošiljatelja sporočila.

4.3.2 RSA

V prejšnjem poglavju smo spoznali algoritem, ki se ukvarja zgolj z izmenjavo ključa in s tem tlakuje pot za šifriranje in dešifriranje s pomočjo simetričnih kriptografskih algoritmov. Med prve prave asimetrične algoritme štejemo algoritem RSA, ki hkrati omogoča šifriranje, dešifriranje in digitalno podpisovanje. Algoritem so leta 1977 razvili Ron Rivest, Adi Shamir in Len Adleman iz univerze MIT. Ime je oblikovano iz inicialk njihovih priimkov. Ob predpostavki uporabe dovolj velikih ključev velja algoritem za zanesljivega in varnega (Hontañón, 2005).

Algoritem RSA danes uporabljajo mnogi komercialni produkti in platforme. Vgrajen je v obstoječe operacijske sisteme Windows, Apple, Sun in Novell. Strojne izvedbe algoritma je moč najti pri mnogih mobilnih telefonih, mrežnih in pametnih karticah. Poleg tega je algoritem vključen v pomembnejše protokole varne internetne komunikacije, na primer S/MIME, SSL in S/WAN. V prihodnosti lahko pričakujemo razširitev na številne nove produkte (RSA Security, 2005).

Algoritem RSA uporablja dva različna ključa, ki sta matematično povezana. Varnost temelji na predpostavki, da privatnega ključa ne moremo izračunati iz javnega. V praksi to pomeni, da je zelo enostavno pomnožiti dve veliki praštevili, medtem ko je obratni postopek, torej iz zmnožka ugotoviti, kateri praštevili smo pomnožili, izjemno zahtevno, če ne nemogoče. Pred samim šifriranjem in dešifriranjem moramo pridobiti javni in privatni ključ oziroma njune

gradnike. Spodnji postopek opisuje izračun parametrov, ki sestavljajo javni in privatni ključ (Rivest et al., 2005):

1. Izberemo 2 neodvisni praštevili p in q,
2. izračunamo njun zmnožek $n = p \cdot q$,
3. izračunamo $\Phi(n) = (p-1) \cdot (q-1)$,
4. izberemo vrednost e pri 2 pogojih:
   - $1 < e < \Phi(n)$,
   - največji skupni delitelj e in $\Phi(n)$ mora biti število 1.
5. Izračunamo vrednost d pri 2 pogojih:
   - $1 < d < \Phi(n)$,
   - $e \cdot d \equiv 1 (\mathrm{mod}\, \Phi(n))$ oz. ko $e \cdot d$ delimo z $\Phi(n)$, mora biti ostanek 1.

Iz zgoraj prikazanega postopka pridobimo ključne sestavine javnega in privatnega ključa. Javni ključ, ki je dostopen na internetu, je sestavljen iz:

- e = enkripcijskega oz. šifrirnega eksponenta,
- n = modula.

Privatni ključ, ki mora biti skrbno varovan, sestavljata 2 gradnika:

- d = dekripcijski oz. dešifrirni eksponent,
- n = modul.

Opozoriti velja, da morajo ostati števila d, p, q in $\Phi(n)$ skrbno varovana in ne smejo priti v roke tretjim osebam. Varnost algoritma temelji na spoznanju, da je privatni parameter d nemogoče izračunati iz javnega ključa, ki vsebuje e in n. Nadalje velja, da je faktorizacija, s katero bi iz števila n dobili praštevili p in q, izredno zahtevna oziroma nemogoča, če le uporabimo dovolj veliki praštevili. V kolikor bi ovrgli omenjena matematična spoznanja, bi varnost algoritma odpovedala.

Pridobili smo števila, ki jih uporabimo za šifriranje in dešifriranje sporočil. Predpostavimo, da želi pošiljatelj berljivo sporočilo BS spremeniti v šifrirano sporočilo $\check{S}S$ tako, da ga bo lahko dešifriral le prejemnik. Zaupnost sporočila zagotovimo s šifriranjem s prejemnikovim javnim ključem. Tako smo prepričani, da lahko le prejemnik opravi proces dešifriranja, saj le on pozna vrednost d, ki je shranjena v njegovem privatnem ključu:

$$\check{S}S = BS^e \bmod n \tag{4.6}$$

Dobimo šifrirano sporočilo $\check{S}S$, ki ga pošljemo prejemniku. Prejemnik opravi obratni postopek z uporabo števila d iz svojega privatnega ključa:

$$BS = \check{S}S^{d} \bmod n \tag{4.7}$$

Zgornji postopek je teoretičen in zato teže razumljiv. Sledi praktičen primer izračuna z uporabo števil majhne velikosti. Rok želi povabiti Katjo na zmenek v sobo 14. Njegova naloga je, da število 14 na tajni način sporoči Katji:

1. Izberemo 2 neodvisni praštevili $p = 11$ in $q = 7$,
2. izračunamo njun zmnožek $n = p \cdot q = 11 \cdot 7 = 77$,
3. izračunamo $\Phi(n) = (p-1) \cdot (q-1) = 10 \cdot 6 = 60$,
4. izberemo vrednost $e = 7$, ki je manjša od $\Phi(n) = 60$, njun največji skupni delitelj pa je število 1,
5. izračunamo vrednost $d = 43$, ki je manjša od $\Phi(n) = 60$. Preverimo tako, da pomnožimo $e \cdot d = 7 \cdot 43 = 301$ in delimo z $\Phi(n) = 60$. Ostanek deljenja je zahtevano število 1.

Izračunali smo vse bistvene sestavine javnega in privatnega ključa (n, e, d). V naslednjem koraku pričnemo s postopkom šifriranja. Število 14 bomo spremenili v šifrirano sporočilo:

$$\check{S}S = 14^{7} \bmod 77 = 42$$

Dobili smo šifrirano sporočilo 42, ki ga pošljemo prejemnici. Katja opravi proces dešifriranja na naslednji način:

$$BS = 42^{43} \bmod 77 = 14$$

Katji smo poslali šifrirano sporočilo »dobiva se v sobi 42«, ki ga je prevedla v pravilno vrednost »dobiva se v sobi 14«. Primer je zelo poenostavljen in ne omogoča večje varnosti. Kot zanimivost lahko povemo, da je navkljub majhnim številom, ki smo jih uporabili pri izračunu, orodje MS Excel popolnoma odpovedalo.

V praksi je potrebno sporočilo dopolniti z naključnimi podatki, da se izognemo premajhnim vrednostim sporočila, s čimer ne bi zagotavljali zadovoljive varnosti. Recimo, da želi Rok sporočiti Katji številko sobe 1. V tem primeru je šifrirano sporočilo enako 1. Enako velja, če bi želeli šifrirati število 0. Poleg velikosti sporočila se pojavi še problem šifrirnega eksponenta e. V primeru, ko je berljivo sporočilo z eksponentom BS^{e} manjše od zmnožka praštevil n,

varnosti ni zadoščeno. Z dodajanjem naključnih podatkov dosežemo še eno pomembno kvaliteto. RSA je deterministično sistem in napadalec lahko z javnim ključem šifrira večje število besed in tako sestavi slovar, ki vsebuje besede in njihove šifrirane kopije. Nato prestreza šifrirana sporočila in jih primerja s svojim slovarjem. Z dodajanjem naključnih podatkov napadalca zmedemo (Coron et al., 2002).

Digitalni podpis RSA

Razvoj informacijskih tehnologij nakazuje, da bo elektronska pošta popolnoma nadomestila klasičen papir z žigom in podpisom. Algoritem RSA med drugim omogoča digitalno podpisovanje sporočil, s čimer zagotavlja identifikacijo pošiljatelja in verodostojnost sporočila. Digitalni podpis se navezuje na pošiljatelja oziroma podpisnika in na vsebino sporočila. Pri tem prejemnik nima možnosti spremembe sporočila, prav tako ne more kopirati podpisa.

Predpostavimo, da želi Rok poslati Katji podpisano sporočilo BS. Najprej mora izračunati podpis P za sporočilo BS z uporabo svojega privatnega ključa d_{Rok} (Rivest et al., 2005):

$$P = BS^{d_{Rok}} \bmod n \tag{4.8}$$

Na takšen način je popolnoma jasno, da lahko P izračuna samo Rok, ker le on poseduje d_{Rok}. Ker želimo, da je sporočilo skrbno varovano pred tujimi očmi in da ga lahko prebere le Katja, opravimo postopek šifriranja z njenim javnim ključem e_{Katja}:

$$\check{S}S = P^{e_{Katja}} \bmod n \tag{4.9}$$

Rezultat je šifrirano sporočilo $\check{S}S$, ki ga pošljemo Katji. Prejemnica šifrirano sporočilo najprej dešifrira s svojim privatnim ključem d_{Katja}:

$$P = \check{S}S^{d_{Katja}} \bmod n \tag{4.10}$$

Katja nadalje z uporabo Rokovega javnega ključa e_{Rok} spremeni podpis P v berljivo sporočilo BS:

$$BS = P^{e_{Rok}} \bmod n \tag{4.11}$$

Tako pride Katja do sporočila BS in njegovega podpisa P, ki nastopata v paru. Na takšen način Rok ne more zanikati pošiljanja sporočila, ker lahko P izračuna samo on. Nadalje Katja

ne more spremeniti BS v BS', ker bi morala v tem primeru kreirati P', kar pa ne more, ker nima Rokovega privatnega ključa d_{Rok}. Zaključimo, da je Katja prejela podpisano Rokovo sporočilo, ki ga ne more spreminjati. Prav tako ne more kopirati njegovega podpisa in ga prilepiti kakšnemu drugemu sporočilu, ker je podpis neposredno povezan s sporočilom.

Varnost algoritma

Varnost algoritma RSA temelji na matematičnem problemu. Zelo enostavno je pomnožiti dve veliki praštevili in tako dobiti zmnožek. Izjemno težko pa je narediti obraten postopek, torej iz zmnožka ugotoviti, kateri praštevili smo pomnožili. Do danes še ni bil odkrit oziroma razvit učinkovit mehanizem, ki bi rešil omenjeni problem. Vendar prav tako ni bilo dokazano, da takšen mehanizem ne obstaja.

V kolikor bi napadalec pridobil ustrezni praštevili (p, q), bi lahko s pomočjo elementov javnega ključa (e, n) izračunal dekripcijski eksponent (d), ki je bistvena sestavina privatnega ključa. Tako bi se v omrežju pojavila dva privatna ključa, ki bi lahko odpirala točno določeno vsebino, seveda namenjeno samo enemu izmed njiju.

Največje število, ki so ga uspeli faktorizirati, je bilo dolgo 663 bitov. Produkt (n), ki je dolg 256 bitov, je možno z navadnim računalnikom faktorizirati v nekaj urah. Za zagotavljanje varnosti mora biti $n > 2048$ *bitov*. Zaključimo, da bo uporaba 4096-bitnih ključev pri asimetrični kriptografiji še zelo dolgo zagotavljala zahtevano varnost (Oppliger, 2005).

Leta 1993 je Peter Shor objavil algoritem, ki temelji na razvoju kvantnih računalnikov in omogoča faktorizacijo velikih števil v polinomskem času. Rešitev je zgolj teoretična in v roku naslednjih 10 do 15 let ne gre pričakovati njene realizacije. V kolikor pa bi takšen računalnik razvili, bi postal algoritem RSA popolnoma nemočen (Bone et al., 2005).

Zaključimo, da je algoritem RSA relativno varen ob predpostavki uporabe dovolj velikih ključev. Vendar so že nakazane rešitve, trenutno zgolj teoretične, ki utegnejo algoritem postaviti pod vprašaj.

4.3.3 ELGAMAL

Naslednji v vrsti pomembnejših asimetričnih algoritmov je ElGamal, ki temelji na Diffie-Hellmanovi izmenjavi ključa. Algoritem je leta 1984 predstavil Taher Elgamal, njegovo jedro pa predstavlja računanje diskretnih logaritmov. V praski se je izkazalo, da sta pri enaki dolžini ključa algoritma RSA in ELGAMAL približno enako varna, medtem ko je RSA hitrejši.

Algoritem ElGamal je možno uporabljati tako za šifriranje in dešifriranje kot za digitalno podpisovanje. V prvem koraku izračunamo javni in privatni ključ. Uporabnik izbere praštevilo p in dve naključni števili g in x iz množice celih števil $\mathbf{Z}_p\{0,1,..., p-1\}$, ki mora biti skrbno izbrana. Nato izračunamo (Schneier, 1996):

$$h = g^x \bmod p \tag{4.12}$$

Z zgornjim izračunom pridobimo javni ključ $(h, g, p, \mathbf{Z}_p)$ in privatni ključ (x). Predpostavimo, da želimo lastniku zgornjega privatnega in javnega ključa poslati berljivo sporočilo BS, ki ga zaradi varnosti spremenimo v šifrirano sporočilo $\check{S}S$. Najprej spremenimo BS v število in izberemo naključno število y. Obe števili (BS, y) morata biti iz množice celih števil $\mathbf{Z}_p$. Nato izračunamo šifrirano sporočilo:

$$\check{S}S_1 = g^y \bmod p \tag{4.13}$$

$$\check{S}S_2 = BS \cdot h^y \bmod p \tag{4.14}$$

Rezultat je iz dveh števil sestavljeno šifrirano sporočilo $(\check{S}S_1, \check{S}S_2)$, ki ga pošljemo prejemniku. Sporočilo dešifrira z uporabo privatnega ključa (x):

$$BS = \check{S}S_2(\check{S}S_1^x)^{-1} \tag{4.15}$$

Pravilnost algoritma lahko preverimo matematično:

$$\check{S}S_2(\check{S}S_1^x)^{-1} = BS \cdot h^y (g^{yx})^{-1} = \frac{BS \cdot g^{xy}}{g^{yx}} = BS \tag{4.16}$$

Digitalni podpis ELGAMAL

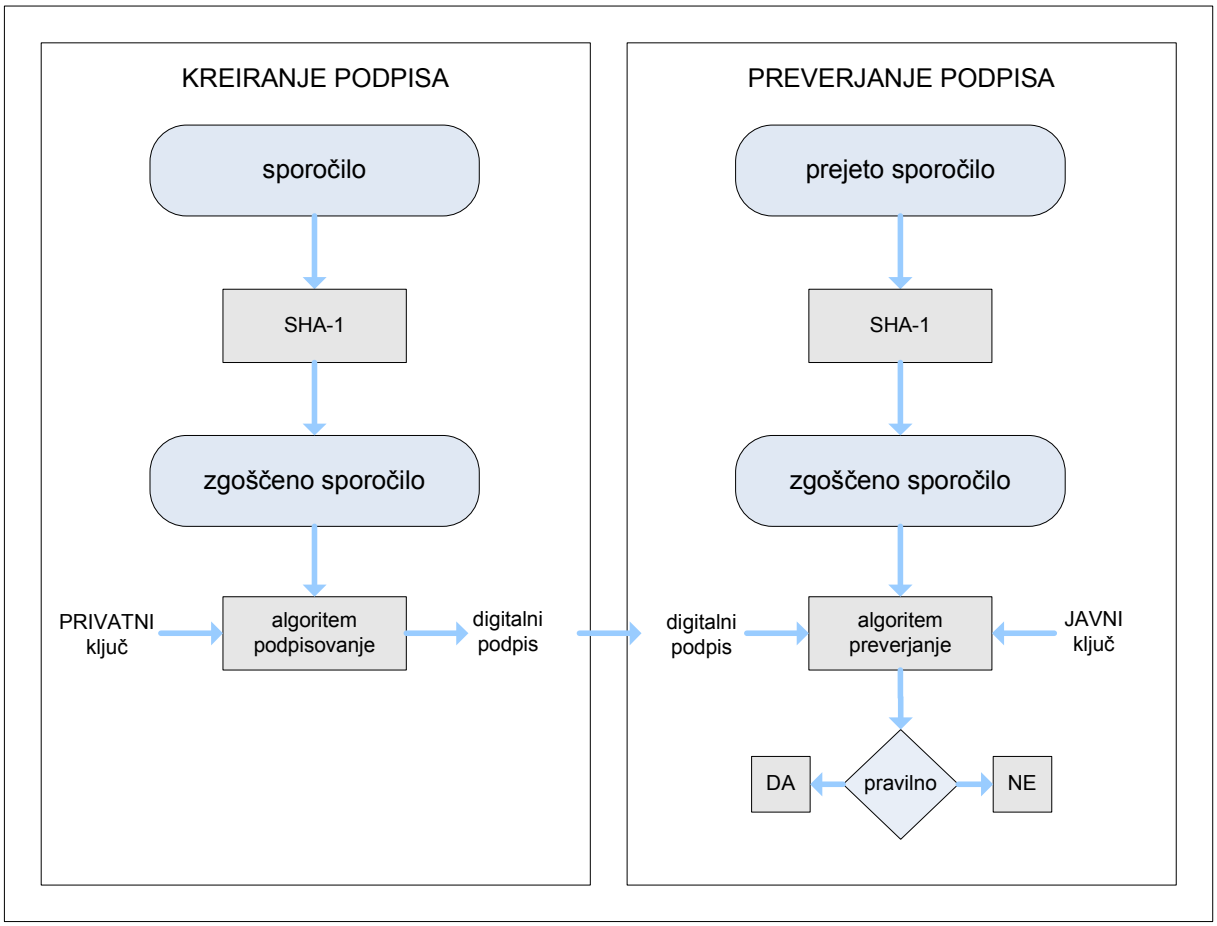
Taher Elgamal je hkrati z razvojem kriptografskega algoritma razvil digitalni podpis, ki prav tako temelji na zahtevnosti računanja diskretnih logaritmov. Namenjen je preverjanju verodostojnosti sporočila in pošiljatelja. V praksi je omenjeni algoritem zelo redko uporabljen, veliko bolj razširjena je ena izmed njegovih variant, imenovana DSA (Digital Signature Algorithm) in bo podrobno predstavljena v nadaljevanju.

4.3.4 DSA

DSA (Digital Signature Algorithm) je algoritem za digitalno podpisovanje, ki ga je na osnovi ElGamalovega digitalnega podpisa razvil in patentiral David W. Kravitz. Algoritem je temeljito testiral institut NIST in ga leta 1994 sprejel kot standard za digitalno podpisovanje dokumentov DSS (Digital Signature Standard). Uporaba je brezplačna in velja za vse države.

Standard opisuje algoritem, ki se uporablja za digitalno podpisovanje. Recimo, da želi Rok poslati Katji sporočilo, ki ohranja nespremenjeno vsebino in jasno definira, kdo je pošiljatelj. Rok sporočilo zgosti s pomočjo funkcije SHA-1 in rezultat šifrira s svojim privatnim ključem. Rezultat skupaj z izvornim sporočilom pošlje Katji, ki ga obdela s funkcijo SHA-1 in dobi zgoščeno sporočilo. Poleg izvornega sporočila je prejela še šifrirano zgoščeno sporočilo, ki ga dešifrira z Rokovim javnim ključem. Rezultata med seboj primerja in v kolikor sta enaka, zaključi, da je digitalen podpis veljaven. To pomeni, da je sporočilo poslal Rok, njegova vsebina pa ni bila spremenjena.

Slika 4.10: Kreiranje in preverjanje digitalnega podpisa



Vir: DSS - FIPS PUB 186-2, 2000, str. 2

Slika 4.10 prikazuje postopek kreiranja in preverjanja digitalnega podpisa. Sporočilo, ki ga želimo podpisati, funkcija SHA-1 zgosti v 160 bitov dolgo sporočilo. Nadalje zgoščeno sporočilo skupaj s privatnim ključem vstopi v algoritem za podpisovanje in rezultat je digitalni podpis, ki ga skupaj s sporočilom pošljemo naslovniku. Prejeto sporočilo s pomočjo zgostitvene funkcije SHA-1 spremeni v zgoščeno sporočilo, ki ga skupaj z digitalnim podpisom in pošiljateljevim javnim ključem obdela s pomočjo algoritma za preverjanje. V kolikor je digitalen podpis veljaven, smo lahko prepričani, da je sporočilo dejansko prišlo od navedenega pošiljatelja (njegov javni ključ) in da njegova vsebina ni bila spremenjena (SHA-1).

Sledi matematična razlaga. Najprej izračunamo javni (p,q,g,y) in privatni (x) ključ. Sporočilo podpišemo na sledeči način (Quisquater et al., 2002):

- izberemo naključno število k ob pogoju $1 < k < q$,
- izračunamo $r = (g^k \bmod p) \bmod q$,
- izračunamo $s = (k^{-1}(SHA-1(BS) + x \cdot r)) \bmod q$, pri čemer je $SHA-1(BS)$ zgoščeno berljivo sporočilo BS.

Rezultat je digitalni podpis v paru (r,s), ki ga prejemnik sporočila preveri:

- izračuna $v = (g^{SHA-1(BS)\cdot s^{-1} \bmod q} \cdot y^{r \cdot s^{-1} \bmod q}) \bmod p) \bmod q$,
- v kolikor je $v = r$, zaključimo, da je podpis veljaven.

4.3.5 ECC

V prejšnjih poglavjih smo opisali asimetrična algoritma (RSA in ELGAMAL), ki sta široko sprejeta in uspešno kljubujeta raznovrstnim napadom ter zadovoljujeta pomembnejše varnostne standarde. Oba omogočata šifriranje, dešifriranje in digitalno podpisovanje. Pojavi se vprašanje, zakaj se spogledujemo z novimi algoritmi, kot je na primer ECC (Elliptic Curve Cryptosystem).

Pravzaprav algoritem ECC ni novo odkritje, saj je bil predstavljen že leta 1985. Neodvisno sta ga razvijala dva kriptografa, Neal Koblitz (University of Washington) in Victor Miller (IBM). V vseh teh letih pa se je okoli eliptičnih krivulj razvila temeljita diskusija o varnosti in učinkovitosti. Ravno slednja je razlog za izredno zanimanje, ki smo mu priča v zadnjem času. Na trgu je možno dobiti različne elektronske pripomočke, kot so ročni računalniki in mobilni telefoni, ki so omejeni s spominom, procesorsko močjo, energijo in pasovno širino. Varnost ni vprašanje in enostavno mora biti zagotovljena. Rešitev je v uporabi eliptične krivulje kot

množice točk, ki rešijo enačbo $y^2 = x^3 + ax^2 + b$. Varnost eliptičnih krivulj temelji na problemu diskretnega logaritma. Prednost je v občutno krajših dolžinah ključev kot pri drugih sistemih. Na primer 160-bitni ključ pri ECC zagotavlja enako varnost kot 1024-bitni ključ pri algoritmu RSA. Na drugi strani pa je implementacija ECC veliko daljša in zahtevnejša kot pri ostalih algoritmih. Temu navkljub je rešitev iz dneva v dan bolje sprejeta in je vključena v številne standarde. Poleg tega jo uspešno uporabljajo mnoga podjetja po svetu (Jurišić et al., 2001).

Bistvena lastnost eliptičnih krivulj je, da lahko definiramo pravila za seštevanje dveh točk na krivulji, pri čemer seštevek prav tako leži na krivulji. Rok in Katja želita varno izmenjati sporočilo in se dogovorita o uporabi eliptične krivulje in na njej ležeče fiksne točke F. Podatkov o eliptični krivulji in točki F ne skrivata, temveč jih javno izmenjata. Rok izbere naključno število R_k, ki je njegov skrbno varovani privatni ključ in izračuna točko na krivulji (Koblitz, 1994):

$$R_t = R_k \cdot F \tag{4.17}$$

To je njegov javni ključ. Katja naredi enako, izbere K_k kot privatni ključ in izračuna javni ključ $K_t = K_k \cdot F$. Predpostavimo, da želi Rok poslati Katji tajno sporočilo. Enostavno izračuna $R_k \cdot K_t$ in uporabi rezultat kot tajni ključ, ki ga uporabi za komunikacijo. Katja na enak način izračuna $K_k \cdot R_t$ in dobi tajni ključ. Da sta ključa resnično enaka, dokažemo s sledečim izračunom:

$$K_k \cdot R_t = K_k \cdot (R_k \cdot F) = (K_k \cdot R_k) \cdot F = R_k \cdot (K_k \cdot F) = R_k \cdot K_t \tag{4.18}$$

Torej drži, da sta ključa ($K_k \cdot R_t = R_k \cdot K_t$) za varno komunikacijo enaka. Uporabimo lahko katerokoli simetrično tehniko šifriranja in dešifriranja. Varnost algoritma temelji na predpostavki, da je izredno težko izračunati k pri znanih F in $k \cdot F$. Na primer, če izberemo praštevilo F reda velikosti 256 bitov, bi za izračun k potrebovali približno 2^{128} operacij. To pomeni, da je lahko velikost ključev in digitalnih podpisov pri uporabi eliptičnih krivulj veliko krajša kot pri drugih algoritmih, seveda ob zagotavljanju enake ravni varnosti (Koblitz, 1994).

5. PROGRAMI IN PROTOKOLI

V prejšnjih poglavjih smo podrobno predstavili glavne kriptografske algoritme. Celovita varnostna rešitev, ki jo imenujemo program oziroma protokol, združuje različne algoritme. Nekateri pomembnejši so predstavljeni v nadaljevanju.

5.1 IPSec

Ena izmed glavnih slabosti internetnega protokola (IP) je, da ne vsebuje mehanizmov za zagotavljanje varnosti podatkov, ki se pretakajo po internetu. Zato so se v preteklih leti razvile mnoge rešitve, ki so se ukvarjale s problemom kriptografije na ravni aplikacij. Z naraščanjem elektronskih transakcij in s tem povezanih potreb po zaščiti podatkov pride do razvoja protokola IPSec (Internet Protocol Security), ki omogoča vzpostavitev varnega komunikacijskega kanala med dvema napravama. Deluje na mrežni ravni in je popolnoma neodvisen od aplikacij. IPSec ni protokol, ki bi narekoval točno določeno uporabo šifrirnega algoritma in ključev, temveč je zasnovan modularno, kar omogoča njegovo odprtost in fleksibilnost. Za izmenjavo tajnega ključa podpira asimetrična algoritma RSA in DSA, za samo šifriranje pa algoritme 3DES, DES, CAST-128, Blowfish in AES. Neokrnjenost podatkov zagotavljata zgoščevalna algoritma MD5 in SHA1.

Druge rešitve, ki bodo predstavljene v nadaljevanju, so bolj specifične in prilagojene delovanju v določnih situacijah in jih ne moremo posploševati.

IPSec torej zagotavlja varnost na mrežni ravni in tako omogoča varnost vsem drugim TCP/IP protokolom in aplikacijam nad njim. Zato ni potrebe po dodatnih varnostnih mehanizmih na višjih ravneh. Postopek vzpostavitve varne komunikacije poteka po naslednjih korakih (Kozierok, 2005):

- dogovor o uporabi varnostnega protokola,
- dogovor o uporabi šifrirnega algoritma,
- izmenjava ključev za šifriranje,
- postopek varne izmenjave sporočil se prične z uporabo zgoraj usklajenih protokolov, algoritmov in ključev.

5.2 SSL/TLS

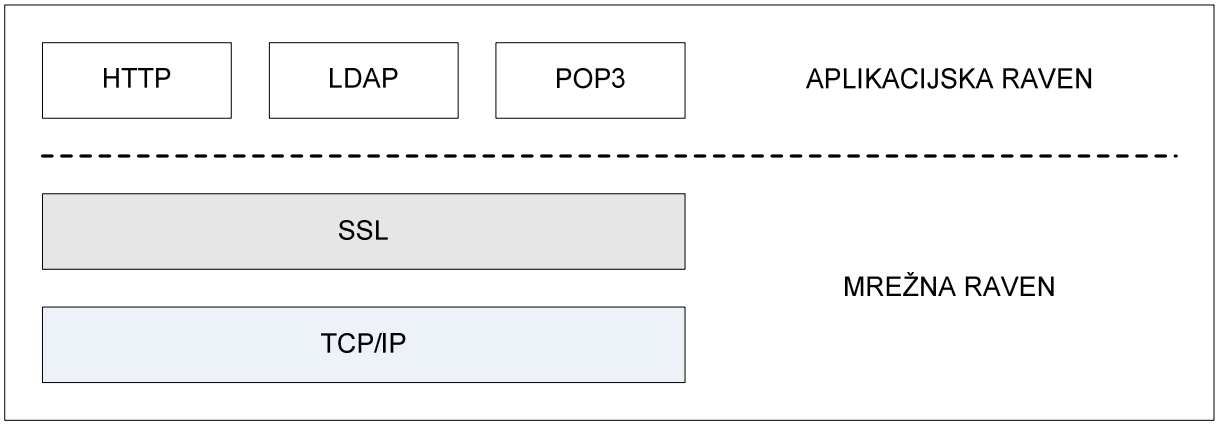
SSL (Secure Socket Layer) je kriptografski protokol, ki omogoča zaščito komunikacijskega kanala na internetu. Protokol je leta 1994 razvil Netscape Communications Corporation. Nekaj let kasneje so ga pomembnejše finančne ustanove (Visa, MasterCard, American Express itd.) sprejele kot standard za elektronsko poslovanje preko interneta. Razvoj je šel naprej in IETF (Internet Engineering Task Force) predstavi protokol TLS, ki je nekoliko izpopolnjena oblika protokola SSL.

Cilj protokola SSL je zagotavljanje zasebnosti in varnosti med dvema aplikacijama, ki komunicirata preko nezavarovanega komunikacijskega kanala. Protokol SSL je umeščen pod

raven aplikacij, kar omogoča njegovo neodvisnost. Torej je varna komunikacija vzpostavljena pred pričetkom izmenjave podatkov na ravni aplikacij.

Protokol SSL srečamo na vsakem koraku varne internetne komunikacije, pri čemer je delež drugih varnostnih rešitev zanemarljiv. Internetna komunikacija poteka skozi različne ravni, preden pride do zahtevanih podatkov, kot je npr. spletna stran. Na najvišji ravni imamo opravka s HTTP, ki v primeru varne komunikacije usmeri zahtevo na SSL. Nasprotno, ko ni potrebe po varni komunikaciji, pride do neposredne usmeritve na TCP/IP in podatke (slika 5.1). Proces vzpostavitve šifrirane komunikacije se prične z rokovanjem, ki je najzahtevnejša faza in uskladi šifrirne algoritme in ključe med strežnikom in odjemalcem. Odjemalčev brskalnik pošlje svoje varnostne nastavitve strežniku, ki poišče ustrezno rešitev in pošlje nazaj svoje digitalno potrdilo z javnim ključem. Odjemalec preveri verodostojnost digitalnega potrdila (overitelj), datum veljavnosti in ustrezno povezavo na spletno stran. Pri protokolu SSL se ponavadi identificira le strežnik, medtem ko je uporabnik anonimen. Možna je tudi izvedba z obojestransko identifikacijo, pri čemer potrebujemo tako strežnikovo kot odjemalčevo digitalno potrdilo. Na podlagi pridobljenih informacij odjemalec kreira simetrični tajni ključ, ki ga zašifrira s strežnikovim javnim ključem. Tako strežnik in odjemalec varno izmenjata simetrični ključ, ki ga uporabljata za šifrirano komunikacijo. Protokol SSL podpira naslednje algoritme: za izmenjavo tajnega ključa uporablja asimetrične algoritme (RSA, Diffie-Hellman, DSA, Fortezza), za samo šifriranje komunikacije pa simetrične algoritme (RC2, RC4, IDEA, DES, 3DES, AES). Za zagotavljanje neokrnjenosti poslanih sporočil uporablja zgoščevalna algoritma MD5 in SHA. Razvijalci so SSL zasnovali modularno, kar omogoča veliko prilagodljivost in razširljivost (Freier et al., 1996).

Slika 5.1: Protokol SSL



Vir: Onyszko, 2004, str. 2

Med brskanjem po internetu se lahko hitro prepričamo o varnosti komunikacije s pogledom na naslov URL, ki se mora začeti s https://. Enako velja za ključavnico v desnem spodnjem kotu

brskalnika, ki mora biti zaklenjena. Komunikacija med odjemalcem in strežnikom je tako ustrezno zaščitena.

5.3 SSH

SSH (Secure Shell) je hkrati program in mrežni protokol, ki omogoča varen terminalski dostop. V preteklosti so bili v uporabi različni protokoli (npr. Telnet, Rlogin, Rsh), ki niso omogočali šifrirane komunikacije. Relativno enostavno je bilo prestreči pomembne podatke in gesla. Dokler so bile računalniške mreže fizično ločene, ni bilo večjih pomislekov. Z razvojem interneta pa vsakomur postane jasno, kako velika je ta varnostna luknja.

SSH je leta 1995 razvil Tatu Ylönen, raziskovalec na tehnični univerzi v Helsinkih, kot odgovor na vdor hekerja, ki je iz fakultetnega omrežja pridobil nekaj tisoč uporabniških imen in gesel (Seifried, 2002). Programska rešitev je bila na začetku brezplačna. Kmalu je ustanovil podjetje SSH Communications Security, ki je začelo tržiti omenjeni produkt. Skupina zanesenjakov je leta 1999 na osnovi zadnje brezplačne verzije razvila OpenSSH, ki ohranja brezplačnost. Do danes je že skoraj v celoti izpodrinil Telnet, Rlogin, Rsh, Ftp in močno prevladuje na trgu konkurenčnih produktov.

Protokol sestavljata strežniški del SSHD in lokalni odjemalec SSH, ki izmenjata javne ključe. Odjemalec pri sebi shrani javni ključ strežnika, strežnik pa javni ključ odjemalca. Ko odjemalec vzpostavi povezavo, dobi od strežnika njegov javni ključ, ki ga primerja z lokalno shranjenim. V naslednjem koraku se dogovorita o simetričnem algoritmu in ključu, ki ga bosta uporabljala za šifriranje. Na koncu strežnik preveri, ali ima odjemalec ustrezen javni ključ.

Obstajata dve različici protokola; SSH-1 in SSH-2, ki uporabljata različne kriptografske algoritme. Novejša različica SSH-2 podpira javna ključa DSA in RSA, za zgoščevanje SHA-1 in MD5 ter za simetrično šifriranje algoritme 3DES, Blowfish, Twofish, IDEA in Arcfour.

5.4 PGP

PGP (Pretty Good Privacy) je leta 1991 razvil Philip R. Zimmermann kot brezplačen program za zagotavljanje varnosti elektronske pošte v duhu zagotavljanja človekovih pravic. Program se je hitro razširil po vsem svetu in avtor je zaradi tega dejanja prišel v navzkriž z ameriškimi oblastmi, ki so omejevale izvoz močnih kriptografskih mehanizmov. Ne glede na to je PGP kmalu postal najbolj razširjen svetovni program za šifriranje elektronske pošte (Zimmermann, 2005).

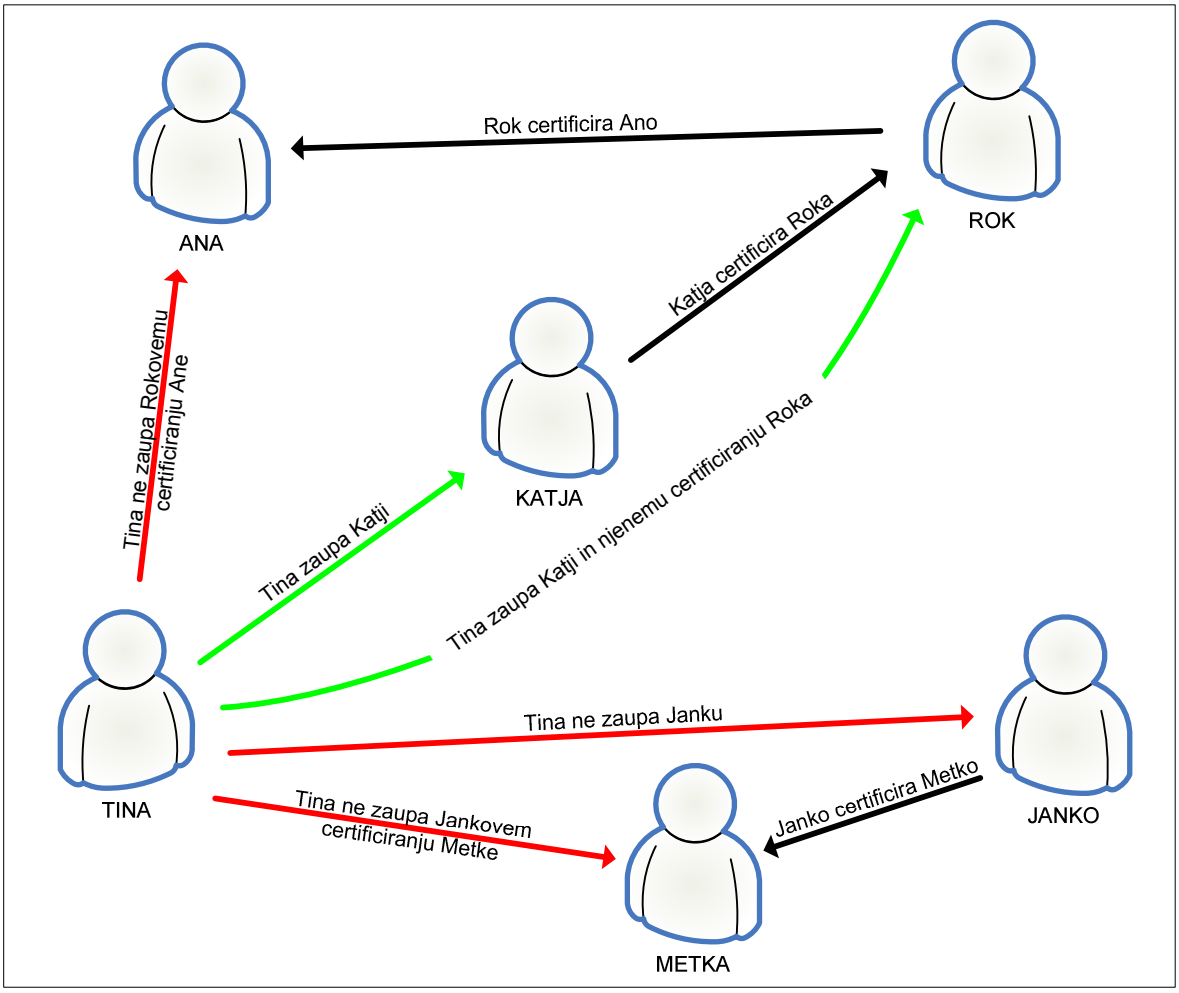
PGP je celovita rešitev, ki s šifriranjem zaščiti tako elektronsko pošto kot datoteke na disku. Uporablja več različnih kriptografskih mehanizmov in dopušča možnost vgraditve dodatnih.

Privzeto PGP uporablja asimetričen algoritem RSA za izmenjavo tajnih ključev in simetrični algoritem IDEA za šifriranje podatkov. PGP zadovolji pomembnejše varnostne zahteve:

- *zaupnost podatkov* zagotovi simetričen algoritem IDEA,
- *neokrnjenost podatkov* dosežemo z uporabo algoritma MD5 (zgoščevanje sporočila),
- *pristnost* omogoča uporaba javnih ključev (certifikati),
- *nezanikanje* dosežemo z digitalnim podpisom.

PGP ne uporablja hierarhije CA (Certificate Authority), temveč se zanaša na zaupanje (t. i. »Web Of Trust«). To pomeni, da uporabniki programa kreirajo svoj javni ključ in ga izmenjajo z drugimi uporabniki. Medsebojno podpišejo ključe in s tem ustvarijo skupino uporabnikov, ki si zaupa (slika 5.2).

Slika 5.2: PGP in mreža zaupanja



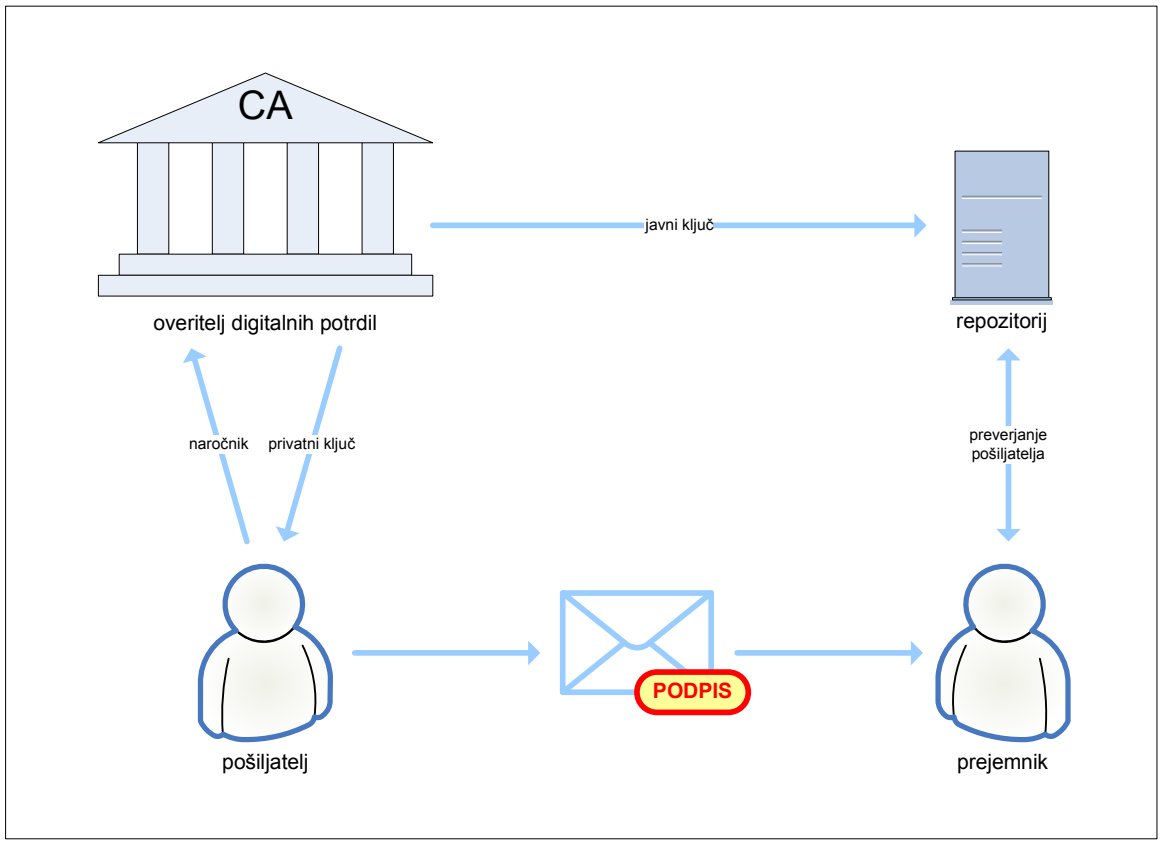
Vir: Nathan et al., 2005, str. 5

Primer: Rok in Katja želita varno komunicirati z uporabo PGP. Rok pošlje svoj javni ključ Katji, ki ga podpiše in shrani na svojem računalniku. Nato Katja pošlje Roku svoj javni ključ in lahko pričneta z varno komunikacijo. Enako naredita Katja in Tina, ki si prav tako zaupata. Recimo, da želi Rok komunicirati s Tino. Rok pošlje Tini svoj javni ključ. Toda Tina ne pozna Roka in ne ve, ali mu lahko zaupa. Ugotovi, da ima Rok svoj javni ključ že podpisan pri Katji in ker ji Tina zaupa, posledično zaupa tudi Roku in varna komunikacija se lahko prične. Očitno je, da Tina verjame zgolj v identiteto Katje in posledično Roka. Vsem drugim akterjem ne zaupa in z njimi ne namerava sklepati kupčij. Povzamemo lahko, da sistem deluje po principu: »Sicer te ne poznam, toda moj dober prijatelj pravi, da si v redu in zato ti zaupam.«

5.5 S/MIME

Tako S/MIME kot PGP sta bila razvita kot protokola za zagotavljanje varnosti pri izmenjavi elektronske pošte (šifriranje in digitalno podpisovanje). Protokola uporabljata enake algoritme in strukture. Bistveno se razlikujeta pri infrastrukturi javnega ključa. S/MIME uporablja CA (Certificate Authority), ki je izbrana in zaupanja vredna agencija (npr. SIGEN-CA), ki izdaja certifikate. Posameznik preverja pristnost certifikatov pri agenciji CA (slika 5.3) in ne pri posameznikih kot v primeru PGP.

Slika 5.3: Infrastruktura javnega ključa



Vir: Savage et al., 2001, str. 18

Na sliki 5.3 je prikazana poenostavljena infrastruktura javnega ključa. Pošiljatelj želi poslati digitalno podpisano pismo prejemniku. Najprej se mora prijaviti na agenciji CA, ki preveri njegove osebne podatke in izda digitalni certifikat (velja daljše obdobje). Tako pošiljatelj pridobi privatni in javni ključ. Privatnega skrbno varuje pri sebi, medtem ko je javni ključ shranjen v javno dostopnih bazah na internetu. Pošiljatelj oblikuje sporočilo in ga digitalno podpiše s svojim privatnim ključem. Prejemnik sporočila s pomočjo pošiljateljevega javnega ključa preveri njegovo identiteto. Primer sicer opisuje digitalno podpisovanje, vendar potekata izmenjava tajnega ključa ali šifriranje podatkov na zelo podoben način.

5.6 GnuPG

GNU Privacy Guard (GnuPG ali GPG) je brezplačno nadomestilo za PGP, ker ne uporablja patentno zaščitenega algoritma IDEA in ga je možno uporabljati popolnoma brez omejitev. Omogočena je uporaba, modifikacije in distribucija pod pogoji licence GNU (Koch, 2005).

GnuPG je orodje za varno komunikacijo, ki omogoča kreiranje ključev (javnega in privatnega), varno izmenjavo ključa, šifriranje in dešifriranje dokumentov ter digitalno podpisovanje.

GnuPG lahko kreira več različnih tipov ključev. Privzeta opcija oblikuje par ključev DSA, ki se uporablja za digitalno podpisovanje. Za šifriranje in dešifriranje podatkov kreira ključa ElGamal. Velikost ključev ne sme biti manjša od 768 bitov. Ključi DSA so navzgor omejeni z velikostjo 1024 bitov, ElGamal pa z velikostjo 2048 bitov. Z večanjem dolžine ključa se povečuje varnosti in zmanjšuje hitrost.

Uporabnika, ki želita varno komunicirati, izmenjata javna ključa. Javni ključ je potrebno uvoziti in potrditi. GnuPG uporablja model zaupanja, ki uporabniku ne omogoča lastnega presojanja. Ključ je možno potrditi le s preverjanjem njegovega prstnega odtisa, kar lahko naredimo samo s pomočjo lastnika ključa. Pri tem lahko uporabimo telefon ali drug komunikacijskih medij, ki omogoča verodostojno komunikacijo. V kolikor se prstna odtisa ujemata, smo lahko prepričani, da imamo pravilno kopijo ključa in varna izmenjava podatkov se lahko prične (Ashley, 2005).

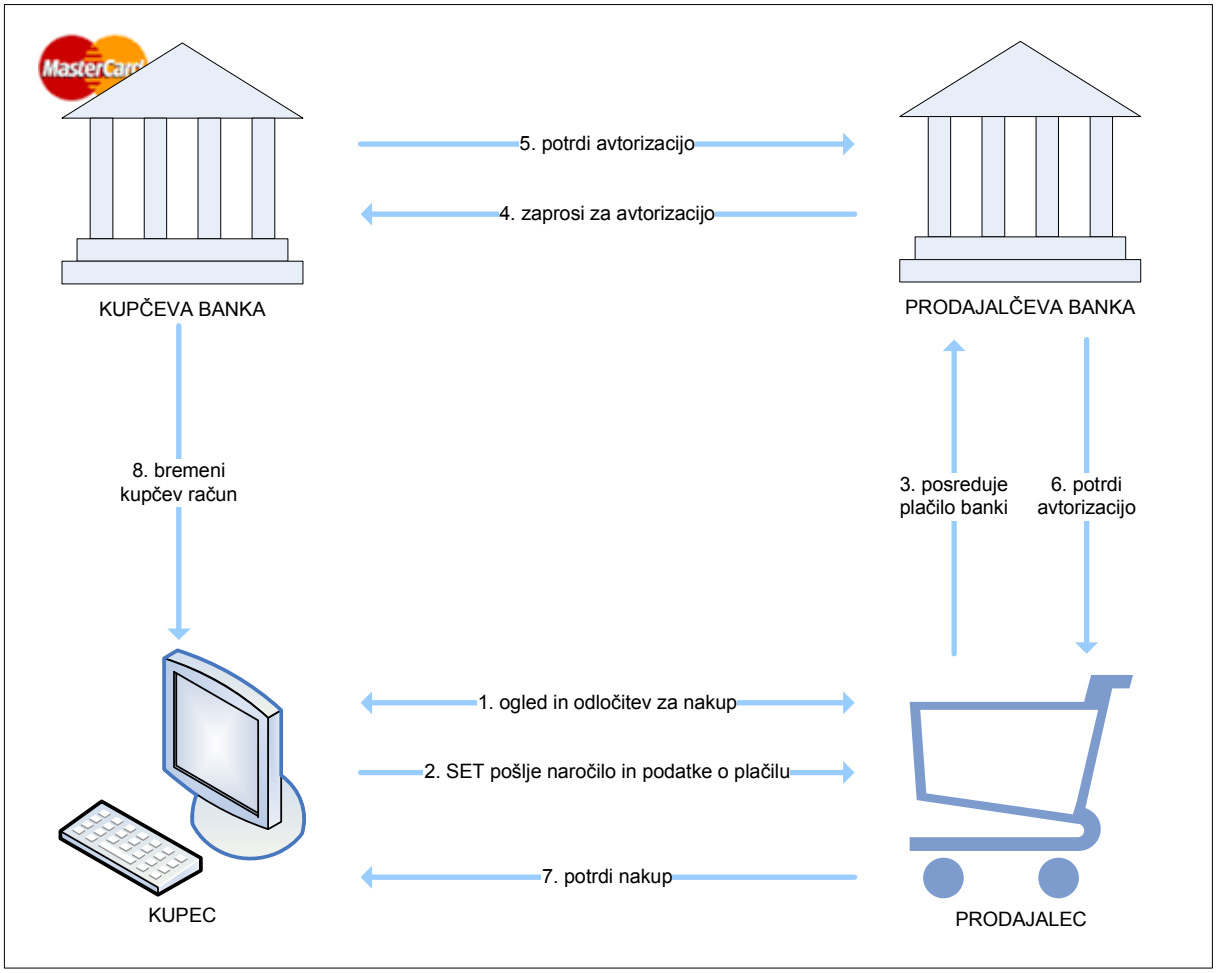
5.7 SET

SET (Secure Electronic Transaction) je protokol za zaščito finančnih transakcij pri nakupih preko interneta. Razvoj protokola sta leta 1996 začela Visa in MasterCard ob pomoči IBM, Microsoft, Netscape, VeriSign in RSA Security. Protokol SET uporablja različne kriptografske metode, ki omogočajo ustrezno identifikacijo in varno izmenjavo podatkov. V

poznih devetdesetih se je začela močna kampanja, ki je SET predstavila kot standard za poslovanje s kreditnimi karticami preko interneta. Kljub temu SET ni uspel postati prvi igralec na tem tržnem segmentu, ker zahteva na strani odjemalca namestitev posebne programske opreme in je relativno drag ter kompleksen za implementacijo na strani trgovcev. Veliko cenejša in enostavnejša rešitev je uporaba SSL, ki ima vodilni delež na trgu.

SET predvideva na strani odjemalca instalacijo *elektronske denarnice*, ki vsebuje osnovne podatke o stranki, njegovi kreditni kartici in digitalni certifikat. Pri elektronskem nakupu pride do medsebojnega preverjanja certifikatov med kupcem, trgovcem in banko (slika 5.4). Protokol omogoča zasebnost in varnost med vsemi navzočimi strankami v procesu.

Slika 5.4: Proces nakupa s protokolom SET



Vir: Boncella, 2000, str. 21

SET zadosti pomembnejšim varnostnim zahtevam po zaupnosti in neokrnjenosti podatkov ter pristnosti in nezanikanju. Pri tem uporablja simetrično in asimetrično kriptografijo. Protokol najprej kreira tajni simetrični ključ, ki ga uporabi za šifriranje sporočila. Podpira šifriranje s simetričnima algoritmoma DES in RC4. Nadalje uporabi asimetričen algoritem RSA za

šifriranje tajnega simetričnega ključa. Oboje pošlje uporabniku, ki najprej s svojim privatnim ključem odklene tajni simetrični ključ, s katerim dešifrira sporočilo (Arikan, 2001).

6. METODA ZA OCENJEVANJE VARNOSTI E-TRGOVIN S PRAKTIČNIMI NAPOTKI

Večji del magistrskega dela predstavljajo algoritmi, ki so sicer implementirani v praksi, vendar si povprečen bralec z njimi ne more kaj veliko pomagati. Sledi poglavje z napotki, kako oceniti varnost nakupa preko interneta, kako varno pošiljati elektronsko pošto in kako varno shraniti podatke na lokalnem disku.

6.1 Varno nakupovanje na internetu

Med spletnim nakupovanjem neprestano izmenjujemo informacije s strežnikom spletne trgovine. Komunikacija poteka preko različnih vozlišč, kjer je možno informacije prestreči. Predstavljajte si številko svoje kreditne kartice, ki prosto potuje čez nekaj deset strežnikov. Da bi zadostili varnosti, moramo šifrirati komunikacijo med našim računalnikom in naslovnim strežnikom. Vendar ali znamo preveriti varnost spletne strani?

Na podlagi teoretičnih spoznanj in lastnih izkušenj definiramo metodo za ocenjevanje varnosti e-trgovin. Na varno komunikacijo postanemo pozorni šele, ko gostitelj od nas zahteva vnos občutljivih podatkov (številka kreditne kartice itd.). Postopek opravimo v petih korakih:

1. Najprej pogledamo URL naslov v glavi brskalnika. Pri nezaščiteni komunikaciji se prične s *http://*, medtem ko pri varni komunikaciji zasledimo dodatek črke s, torej *https://*.

2. Ključavnica v spodnjem desnem kotu brskalnika (pri nekaterih izvedbah v levem kotu) mora biti zaklenjena. To ni zgolj slika ključavnice, temveč omogoča dvoklik, ki odpre okno s podrobnostmi o varnosti spletne strani.

3. Na spletni strani poiščemo nalepko izdajatelja certifikata (npr. VeriSign), ki je interaktivna in nas preusmeri na spletno stran overitelja, kjer pridobimo več informacij o identiteti trgovca.

4. Trgovca preverimo v spletnih iskalnikih. Pri tem si pomagamo z negativnim izrazoslovjem. V iskalnik napišemo ime trgovca in besede, kot so *»fraud«*, *»fraud directory«*, *»betray«*, itd. V kolikor ne najdemo pomembnejših obremenilnih vsebin, smo na dobri poti varnega nakupovanja.

5. Preverimo poslovanje podjetja, ki je nosilec spletne trgovine. Pomagamo si z javno dostopnimi bazami ali orodji za preverjanje bonitet poslovanja (npr. iBON).

Omenjene zahteve si najlažje predstavljamo s predstavitvijo na konkretnem primeru. Preverimo varnost nakupa pri spletnem trgovcu z računalniško opremo EnaA.com (http://www.enaa.com).

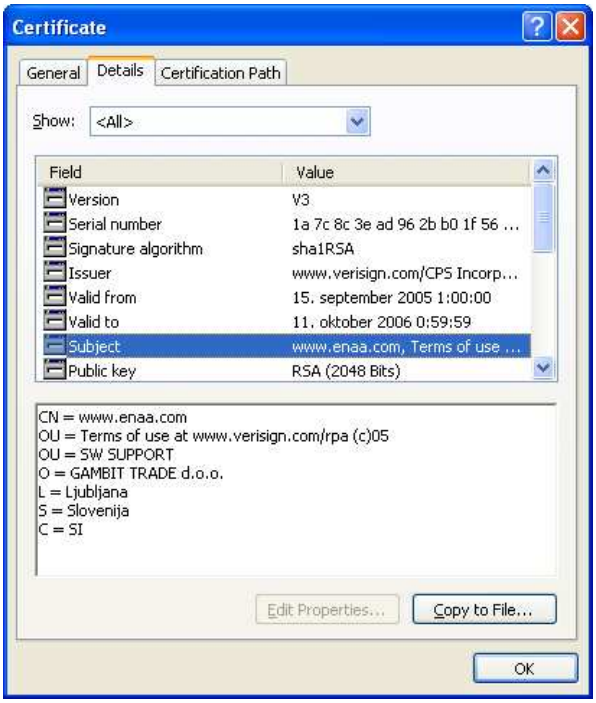
1. Pri klikanju po raznovrstnih povezavah v omenjeni spletni trgovini se naslov vedno začne s *http://*. Ko ogled preide v željo po nakupu, kliknemo na košarico, ki nas preusmeri na varno stran. Vidimo dodatek črke s (*https://*), ki pomeni vzpostavitev varne komunikacije med nami in ciljnim strežnikom.

2. V spodnjem desnem kotu brskalnika poiščemo zaklenjeno ključavnico (slika 6.1), ki je neposredno povezana z naslovom *https://*.

Slika 6.1: Varnostna ključavnica

Dvoklik na ključavnico razkrije pomembne podatke (slika 6.2) o izdajatelju certifikata VeriSign (zaupanja vredna institucija), nosilcu certifikata (podjetje Gambit Trade d.o.o.), šifrirnem algoritmu (RSA z uporabo 2048-bitnega ključa), veljavnosti certifikata itd.

Slika 6.2: Digitalno potrdilo EnaA



3. V tretjem koraku poiščemo interaktivno nalepko izdajatelja certifikata. Na skrajno spodnjem delu spletne strani se nahaja povezava »Vaša zasebnost« in na naslednji strani nalepka VeriSign Secured (slika 6.3).

Slika 6.3: Interaktivna nalepka

Povezava interaktivne nalepke nas preusmeri na spletno stran izdajatelja certifikata *VeriSign*, kjer pridobimo nekaj dodatnih informacij o nosilcu spletne strani in varnosti komunikacije. Poleg tega stran omogoča prijavo zlorabe certifikata.

4. V četrtem koraku s pomočjo spletnega iskalnika *Google* preverimo morebitne obremenilne vsebine omenjene strani. Ne zasledimo relevantnih zadetkov, kar pomeni, da smo na dobri poti varnega nakupovanja.

5. V zadnjem koraku s pomočjo orodja za preverjanje bonitet poslovanja iBON preverimo poslovanje podjetje Gambit Trade d.o.o. Ugotovimo, da podjetje dobro posluje, ustvarja pozitiven denarni tok, nima blokiranih transakcijskih računov itd. Na podlagi vseh pridobljenih informacij zaključimo, da omogoča spletna stran http://www.enaa.com varno nakupovanje.

6.2 Digitalno potrdilo

V današnjem hitro razvijajočem se svetu e-poslovanja je ključnega pomena elektronska identifikacija podjetij in posameznikov, s katerimi sklepamo posle. Digitalno potrdilo združuje javni ključ z identitetno njegovega lastnika.

Koncept javnega ključa, ki je bil predstavljen v teoretičnem delu naloge, je tesno povezan z digitalnim potrdilom. Če želimo pošiljati šifrirano elektronsko pošto in jo digitalno podpisovati, moramo pridobiti ustrezno digitalno potrdilo.

Digitalno potrdilo (slika 6.4) je možno pridobiti na http://www.sigen-ca.si/, kjer domuje SIGEN-CA, izdajatelj kvalificiranih digitalnih potrdil Centra Vlade RS za Informatiko (CVI). Za fizične osebe je pridobitev certifikata brezplačna.

Slika 6.4: Digitalno potrdilo SIGEN-CA

Pridobiti je možno osebna ali spletna kvalificirana digitalna potrdila. Priporočamo naročilo spletnih digitalnih potrdil, ki omogočajo varno spletno komuniciranje po protokolih SSL in TLS, varno pošiljanje elektronske pošte po protokolu S/MIME, šifriranje in dešifriranje podatkov, digitalno podpisovanje ter izkazovanje istovetnosti imetnika. Nenazadnje omogočajo uporabo določenih storitev, za katere se zahteva uporaba omenjenih digitalnih potrdil (npr. elektronska oddaja dohodnine). Postopek naročila in prevzema certifikata zahteva nekaj aktivnosti in traja več dni, vendar je načeloma prijazen do uporabnika.

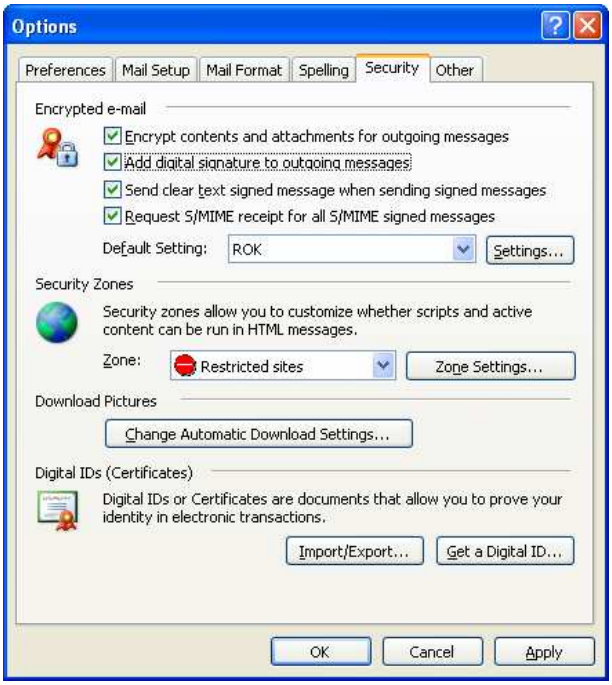
SIGEN-CA uporablja digitalni certifikat X.509v3. To je format digitalnega potrdila, ki ga enostavno povedano uporabljajo vsi. Pri tem je pomembno poudariti, da digitalni certifikat zagotavlja zgolj identifikacijo in ne dobre namere. Vsakdo lahko pridobi digitalno potrdilo za spletno trgovino in prične zbirati številke naših kreditnih kartic. Sicer se je identificiral in vemo, kdo je, vendar ali mu lahko zaupamo?

6.3 Šifriranje in digitalno podpisovanje elektronske pošte

V prejšnjem poglavju smo nakazali možnost pridobitve digitalnega potrdila, ki ga imamo shranjenega na računalniku. Potrdilo lahko kasneje uvozimo v različne aplikacije, na primer v MS Outlook, s čimer omogočamo šifriranje in digitalno podpisovanje elektronske pošte.

Zaženemo MS Outlook 2003 in odpremo meni *»Tools«* in nato *»Options«*. Izberemo zavihek »*Security«*, kjer uvozimo digitalni certifikat *»Digital ID's - Import/Export«* (slika 6.5):

Slika 6.5: Nastavitve varnosti e-pošte



Znotraj istega zavihka poiščemo polje *»Encrypted e-mail«*, ki ponuja nabor več opcij (slika 6.5):

- *»Encrypt contents and attachments for outgoing messages«*. Vključena opcija pomeni, da bodo vsa naša sporočila in njihove priponke šifrirana. Vsebino bo lahko prebral le prejemnik.
- *»Add digital signature to outgoing messages«*. Omogoča digitalno podpisovanje elektronske pošte. Prejemniku pošte omogoča, da ugotovi, kdo je dejanski pošiljatelj in da vsebina sporočila med prenosom ni bila spremenjena.
- *»Send clear text signed message when sending signed messages«*. Omogoča prejemnikom z odjemalcem pošte, ki ne podpirajo protokola S/MIME, da sporočilo preberejo brez verifikacije in podpisa.
- *»Request S/MIME receipt for all S/MIME signed messages«*. Zahteva po povratni informaciji od prejemnika za podpisana sporočila S/MIME.
- Gumb *»Settings«*. Omogoča izbiro različnih algoritmov za šifriranje in zgoščevanje (slika 6.6).

Slika 6.6: Podrobne nastavitve algoritmov

Smiselno je pustiti privzete nastavitve in že lahko pošiljamo šifrirano in digitalno podpisano elektronsko pošto. Za šifriranje komunikacije S/MIME omogoča uporabo kateregakoli izmed treh simetričnih algoritmov: 3DES (168 bitov), DES (56 bitov) in RC2 (od 40 do 128 bitov). Za digitalno podpisovanje uporablja zgoščevalna algoritma SHA1 in MD5.

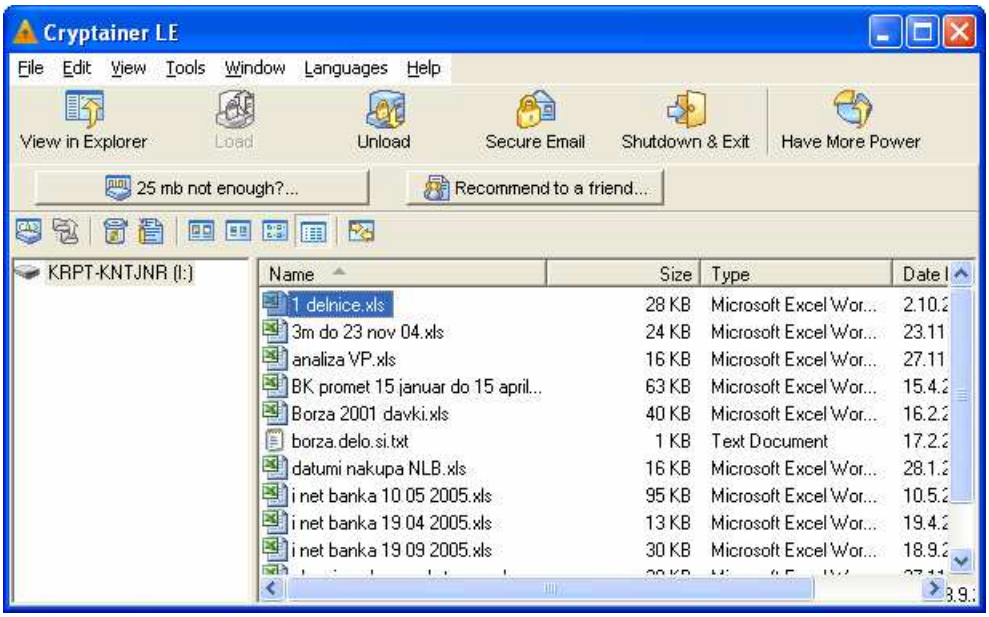
6.4 Zaščita datotek na osebnem računalniku

Na trgu obstaja večje število aplikacij za šifriranje podatkov na disku. Ena najboljših rešitev je Entrustov Entelligence (www.entrust.com), ki ga je možno uporabljati skupaj z digitalnim potrdilom. Uporaba je možna le ob nakupu programske opreme.

Nekoliko enostavnejša rešitev je Cypherixov Cryptainer LE (www.cypherix.co.uk), ki je brezplačen in časovno neomejen (slika 6.7). Z njim lahko varno shranjujemo podatke na našem računalniku do skupne velikosti 25 MB. Če to ne zadošča, je proti plačilu možno program nadgraditi z večjo kapaciteto. V nadaljevanju predstavljamo osnovno verzijo, ki jo naložimo iz zgoraj omenjene spletne strani. Instalacija programa je prijazna do uporabnika in nas med samim postopkom vodi od kreiranja gesla do navideznega diska velikosti 25 MB.

Cryptainer LE za šifriranje uporablja 128-bitni simetrični algoritem Blowfish, ki ga je razvil Bruce Schneier in ponudil v brezplačno uporabo. Nekoliko naprednejše verzije Cryptainer ME, PE in 6.0 uporabljajo celo 448-bitno verzijo omenjenega simetričnega algoritma, kar zagotavlja odlično zaščito pred vsemi do sedaj znanimi napadi.

Slika 6.7: Cryptainer LE (zaščita podatkov na disku)



Aplikacija deluje po principu *»zabojnika«* kot virtualnega diska, v katerega premikamo občutljive datoteke, ki jih želimo zaščititi. Vsebina zabojnika je šifrirana in ko aplikacijo ugasnemo, disk izgine. Do vsebine dostopamo s ponovnim zagonom aplikacije in vnosom gesla. Če smo geslo pozabili, bo vsebina ostala večno skrita.

Vsebina zabojnika je avtomatično šifrirana. Lahko pa posamezno datoteko šifriramo s ključem in jo shranimo v navadno mapo ali pošljemo po elektronski pošti. Na drugi strani prejemnik z istim ključem (geslom) dešifrira datoteko in krog varne komunikacije je sklenjen.

7. VARNOST SLOVENSKIH E-TRGOVIN

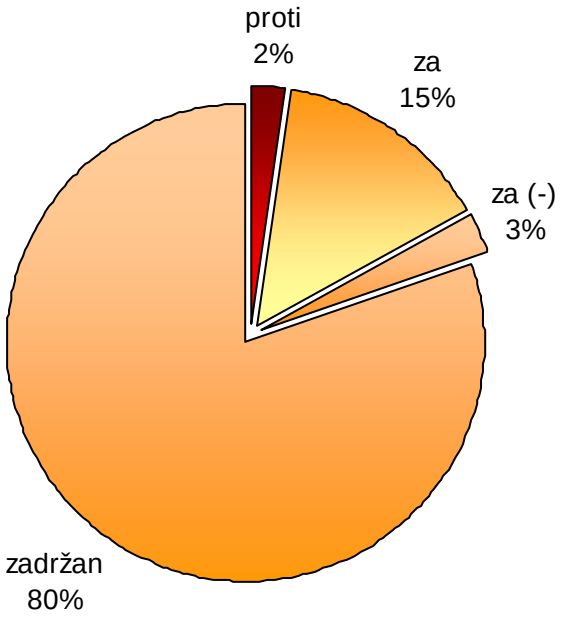
V empiričnem delu magistrske naloge sledi analiza varnosti slovenskih e-trgovin. Trgovine smo izbrali s pomočjo iskalnikov na podlagi ključne besede *»spletna trgovina«*. Prišli smo do števila 344, vendar smo naknadno ugotovili, da besedi spletna trgovina ustreza le 62 % omejenih zadetkov, kar pomeni 212 spletnih trgovin, ki so predmet naše analize. Slednje omogočajo nakup izdelkov iz domačega naslonjača, medtem ko so preostale bolj ali manj namenjene marketingu in usmerjanju potencialnih kupcev v klasične trgovine.

Vsako spletno trgovino posebej smo obiskali in simulirali nakup naključnega izdelka vse do zadnjega koraka, potrditve nakupa. Pri 70 % trgovin je bilo potrebno pred nakupom izdelka opraviti registracijo uporabnika, pri drugih to ni bilo potrebno. V vseh fazah, tako registracije kot nakupa, smo analizirali vzpostavitev šifrirane komunikacije med svojim računalnikom in ciljnim spletnim strežnikom. Uporabili smo metodo ocenjevanja varnosti spletnih trgovin iz prejšnjega poglavja. Vsako spletno trgovino smo opisali na podlagi naslednjih spremenljivk:

- področje (npr. avtomobilizem, darila, elektronika, itd.),
- ime trgovine in kratek opis prodajnega programa,
- spletni naslov (URL),
- varnost prijave (šifrirana prijava; možni odgovori so DA, NE in / , spletna trgovina ne omogoča prijave),
- varnost nakupa (šifriran nakup, možna odgovora sta DA in NE),
- protokol (uporabljen protokol šifriranja),
- javni ključ (javni ključ in njegova velikost),
- CA (navedba izdajatelja digitalnega potrdila),
- priporočilo nakupa (možni odgovori so ZA, ZA(-), PROTI, ZADRŽAN),
- opomba (kratek komentar oziroma utemeljitev priporočila nakupa).

Celotno tabelo si je možno ogledati v prilogi. V splošnem je najbolj zanimiva spremenljivka »priporočilo nakupa« (slika 7.1).

Slika 7.1: Priporočilo nakupa v slovenskih spletnih trgovinah

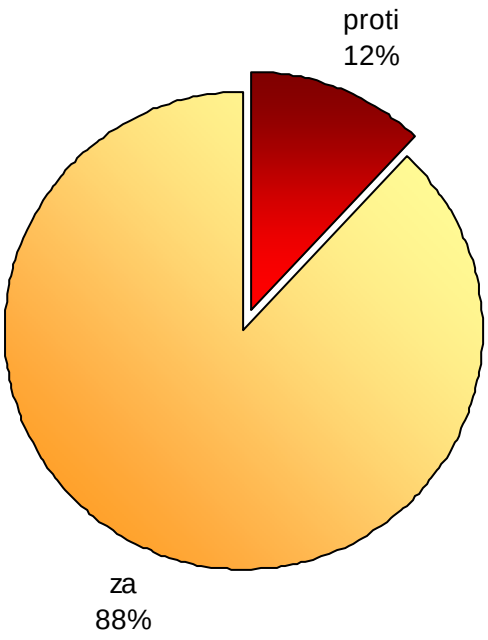


Ugotavljamo, da je le 15 % slovenskih trgovin ustrezno poskrbelo za varnost nakupa. Če upoštevamo še 3 % trgovin, kjer je priporočilo nakupa z zadržkom (zadržek zaradi nešifrirane prijave, ki omogoča zlorabo uporabniškega imena in gesla), govorimo o 18 % varnih spletnih trgovinah.

Velika večina, 80 % spletnih trgovin, je bila ocenjena z zadržanim priporočilom nakupa. To so trgovine, ki ne uporabljajo varnostnih mehanizmov, vendar prav tako ne omogočajo plačila s kreditnimi karticami. Gre za klasično naročanje in plačilo po povzetju ali nakazilo na prodajalčev transakcijski račun. To pomeni, da ni nevarnosti zlorabe kreditne kartice, lahko pa se nepridiprav poigra in se vključi v proces nakupa ter nam popravi število naročenih izdelkov z npr. 1 na 10. Možna je povzročitev kakšne neprijetne situacije, večje škode pa ne. Vprašanje pa je, ali lahko takšne trgovine sploh imenujemo spletne?

Veliko pozornost je potrebno posvetiti spletnim trgovinam, ki so dobile negativno oceno (2 %). To so trgovine, ki omogočajo vnos številke kreditne kartice brez ustrezne zaščite ali pa izdajo digitalno potrdilo same sebi. Nakup v takšni spletni trgovini ocenjujemo kot potencialno nevaren. Če se omejimo zgolj na 42 spletnih trgovin, ki omogočajo plačevanje s kreditnimi karticami, ugotovimo, da smo zaradi pomanjkljive varnosti kar pri 12 % odsvetovali nakup (slika 7.2).

Slika 7.2: Priporočilo nakupa s kreditno kartico



Poudarimo naj, da je predmet analize zgolj varnost nakupa in ne ocenjevanje ponudbe, podobe in konkurenčnosti spletne trgovine. Pozitivna ocena priporočila nakupa pomeni, da spletni nakup ustreza varnostnim zahtevam, kar pa še ni zagotovilo dobrega in kvalitetnega nakupa.

Zanimivo je, da vseh 18 % oziroma 37 spletnih trgovin, ki omogočajo varno spletno nakupovanje, uporablja varnostni protokol SSL in asimetričen ključ RSA, predvsem dolžine 1024 bitov. Drugih rešitev ne najdemo, kar nakazuje veliko razširjenost protokola SSL.

Omenjene trgovine uporabljajo digitalna potrdila različnih zaupanja vrednih organizacij, pri čemer prevladuje Thawte (49 %), sledita VeriSign (24 %) in Equifax (24 %).

V nadaljevanju sledi predstavitev različnih področij slovenskih spletnih trgovin s poudarkom na določenih konkretnih trgovinah. Analiza vseh spletnih trgovin se nahaja v prilogi.

7.1 Avtomobilizem

V kategorijo avtomobilizma smo uvrstili 7 trgovin. Izpostaviti velja trgovino BITEA (pnevmatike; http://trgovina.lmbitea.si/trg/kum), ki omogoča vnos kreditne kartice brez ustrezne zaščite. Nakup v omenjeni trgovini odsvetujemo. Druge trgovine so dobile zadržano priporočilo nakupa, ker omogočajo zgolj naročanje in plačilo po povzetju. Kot zanimivost omenimo, da spletna trgovina Suzuki Odar (avtomobili, motorna kolesa, oprema; http://www.trgovec.net/suzuki) omogoča nakup osebnega vozila ali motornega kolesa preko interneta. Splošna ocena varnosti trgovin v omenjeni kategoriji je nezadovoljiva.

7.2 Darila

Analizirali smo 9 trgovin na področju ponudbe daril. Svetla izjema je spletna trgovina Založbe Rokus (darila; http://www.darila.com), ki omogoča varno nakupovanje in nakazuje zanimivo rešitev za informacijsko manj spretne trgovce, saj uporablja eksterni plačilni sistem (kastor.eon.si). Povedano z drugimi besedami, spletna trgovina je navadna html stran, ki nas ob odločitvi za nakup preusmeri na skrbno varovan strežnik, kjer do konca izpeljemo postopek nakupa. Pri tem je pomembna ugotovitev, da podatki o naši kreditni kartici zaobidejo trgovca in so posredno preko eksternega plačilnega sistema avtorizirani na banki. Trgovec zgolj dobi zeleno luč, da je avtorizacija uspešna in da lahko odpošlje naročeno blago. Druge trgovine v segmentu daril smo ocenili z zadržkom, ker omogočajo zgolj naročanje in plačilo po povzetju. Podobno kot v segmentu avtomobilizma zaključimo, da je varnost nezadovoljiva.

7.3 Elektronika

Na področju elektronike najdemo, kot je pričakovati, večje število spletnih trgovin. Med analizo 22 trgovin si bodečo nežo zasluži spletna trgovina Fonex (antenski in satelitski sistemi, avdio-video oprema in ostala elektronika; http://www.efonex.com), ki omogoča nezaščiten vnos številke kreditne kartice, zato spletni nakup odsvetujemo. Nadalje v omenjenem segmentu beležimo 4 trgovine (18 %), kjer je varnost nakupa ocenjena kot pozitivna. Pri 17 trgovinah (77 %) smo priporočilo nakupa ocenili z zadržkom, ker je omogočeno zgolj naročanje in plačilo po povzetju. Prikazana struktura priporočil nakupa

ustreza povprečju vseh segmentov, kjer je prav tako 18 % pozitivnih ocen varnosti in približno 80 % zadržanih priporočil nakupa.

7.4 Erotika

Na področju erotike v Sloveniji deluje 6 specializiranih spletnih trgovin. Pri vseh je bilo priporočilo nakupa ocenjeno z zadržkom, ker gre za navadne html strani, ki omogočajo zgolj naročanje in plačilo po povzetju. Vse trgovine brez izjeme posvečajo veliko prostora pisanju o diskretnosti nakupa in nevtralnem embaliranju. To je zelo moteče, ker niti malo ne poskrbijo za elektronsko varnost in s tem dejansko diskretnost nakupa. V informacijski družbi velja, da je fizično zaščito relativno lahko zagotoviti, medtem ko je zaščito informacij zelo težko zagotoviti.

7.5 Fotografija, grafika

Pod drobnogled smo vzeli 14 spletnih trgovin s področja fotografije in grafike. Pohvalo zasluži samo ena trgovina, in sicer Fotomarket (digitalni in klasični fotoaparati ter dodatna oprema; http://www.fotomarket.net), ki omogoča pravo internetno nakupovanje pri zagotavljanju popolne varnosti. Presenetljivo je, da preostalih 13 trgovin omogoča zgolj navadno naročanje in plačilo po povzetju, zato smo podali oceno »zadržan«. Ugotovitev je presenetljiva, ker se foto oprema, predvsem digitalna fotografija, spogleduje z računalništvom in elektroniko – posledično bi pričakovali boljšo zaščito nakupov.

7.6 Glasba, video

V omenjeni kategoriji se nahaja 7 spletnih prodajaln. Omeniti velja, da je možno določeno glasbeno ali video opremo najti tudi v drugih kategorijah (npr. računalništvo). Izpostavimo trgovini Siddharta (albumi in drugi artikli, povezani s skupino; http://www.blagajna.com/siddharta) in Lastra Company (klasični glasbeni instrumenti; http://www.lastracom.com), ki sta dobili pozitivno oceno. Slednja, Lastra Company, nima zaščitene prijave uporabnika, kar omogoča zlorabo uporabniškega imena in gesla. Stran že vsebuje zaščito nakupa, zato bi lahko v nekaj minutah dodali še zaščito prijave in varnost ne bi bila več vprašljiva. Preostala podjetja v segmentu so dobila oceno »zadržan«, ker tako kot 80 % drugih slovenskih spletnih trgovin omogočajo zgolj naročanje in plačilo po povzetju.

7.7 Kataloška prodaja

S kataloško prodajo se pri nas ukvarja 6 spletnih trgovin. Od tega smo 50 % trgovin ocenili z zadržkom, ker omogočajo zgolj naročanje in plačilo po povzetju. Pozitivno smo varnost nakupa ocenili pri trgovini JACQUELINE Boutique (spalne srajčke; http://www.impel-

bohinj.si/shop), pozitivno z zadržkom (nezavarovana prijava) pa Neckermann (kataloška prodaja; http://www.neckermann.si). Kritiko si zasluži trgovina TV PRODAJA (kataloška prodaja; http://www.top1.tv), ker uporablja digitalno potrdilo neznanega izdajatelja (Kupi d.o.o.) in ne omogoča zaščitene prijave v trgovino.

7.8 Knjige, revije

Na področju knjig in revij smo analizirali 19 spletnih prodajaln. Med njimi jih je 26 % dobilo pozitivno oceno varnosti nakupa, kar segment knjig in revij uvršča med nadpovprečno varne. Na drugi strani je potrebno opozoriti na potencialno nevarnost nakupa v knjigarni s ponesrečenim spletnim naslovom Prešernova družba (knjige in revije; http://www.prdr.com). Družba oziroma trgovina je sama sebi izdala digitalno potrdilo, pa še temu je potekel rok trajanja. Poleg tega spletna stran uporablja nezadovoljivo dolžino ključa RSA 512 bitov in nakup odsvetujemo. Preostalih 68 % trgovin je dobilo oceno »zadržan«, ker omogočajo zgolj naročanje in plačilo po povzetju.

7.9 Lepota in zdravje

Analizirali smo 13 trgovin s področja lepote in zdravja. Tri trgovine (23 %) so dobile pozitivno oceno varnosti nakupa. To so Aurea (naravna kozmetika; http://www.btc-city.com/aurea), Flegis (ustna higiena; http://www.flegis.si) in Mediteranea (vrhunski izdelki za nego; http://www.mediteranea.si). Slednji dve uporabljata eksterni plačilni sistem kastor.eon.si, medtem ko je prva trgovina Aurea umeščena v spletno nakupovalno središče www.btc-city.com, ki nakazuje varno prihodnost spletnega nakupovanja. Preostalih 77 % trgovin v tem segmentu je dobilo zadržano priporočilo nakupa, ker omogočajo le naročanje preko interneta. Segment lepote in zdravja v splošnem uvrščamo v nadpovprečno varne, poleg tega ne beležimo trgovine, v kateri bi odsvetovali nakup.

7.10 Oblačila, obutev, nakit

Analizirali smo varnost 8 trgovin z oblačili, obutvijo in nakitom. Pozitivno smo ocenili samo spletno prodajalno Benetton (moda za mlade in odrasle; http://www.btc-city.com/benetton), ki deluje v sklopu virtualnega BTC City. Prednost takšne rešitve je, da se prodajalec ukvarja zgolj s svojo osnovno dejavnostjo, računalniški del pa prepusti ustrezno usposobljenim strokovnjakom. Preostalih 7 trgovin (88 %) smo ocenili z »zadržkom«, ker jih le s težka imenujemo prave spletne prodajalne. Segment oblačil, obutve in nakita glede varnosti sodi v zlato sredino ocenjevanih segmentov.

7.11 Optika

V omenjeno kategorijo smo uvrstili zgolj dve trgovini: Optika Medvešek (kontaktne leče; http://www.optika-medvesek.si) in Optimist optika (optični pripomočki; http://www.optimist-optika.com), ki omogočata zgolj naročanje preko interneta in plačilo po povzetju. Posledično sta prodajalni dobili oceno »zadržan«.

7.12 Pirotehnika

Podobno kot v prejšnjem segmentu imamo med pirotehničnimi trgovinami le 2 primera. Trgovina Veronika (pirotehnika; http://www.povzarija.net/pirotehnika) je dobila zadržano priporočilo nakupa, ker omogoča zgolj naročanje in plačilo po povzetju, medtem ko je trgovina Piromarket (pirotehnika; http://www.piromarket.com) dobila pozitivno oceno, ker uporablja eksterni plačilni sistem (eSiOL), ki popolnoma poskrbi za varnost. Statistično gledano je segment pirotehnike na področju varnosti zmagovalec, vendar je reprezentativnost vzorca zaradi majhnega števila trgovin nezadovoljiva.

7.13 Pisarniški material

V kategoriji pisarniškega materiala smo analizirali 7 spletnih prodajaln. Slika segmenta je izredno monotona, saj je vseh 7 trgovin dobilo oceno nakupa »zadržan«. Vse so narejene po enakem kopitu in kot že mnogokrat povedano, omogočajo zgolj naročanje in plačilo po povzetju.

7.14 Računalništvo

Na področju računalniških trgovin smo analizirali kar 40 spletnih trgovin. Večje število trgovin v segmentu je pričakovano in zagotavlja reprezentativnost vzorca. Na podlagi rezultatov lahko utemeljimo pričakovanja o nadpovprečni varnosti nakupov. Kar 7 trgovin je dobilo pozitivno oceno in še nadaljnjih 3, ki so dobile pozitivno s kakšno pomanjkljivostjo (npr. nezaščitena prijava). Skupaj imamo v segmentu računalništva 10 trgovin (25 %), kjer nakup načeloma podpiramo. Izpostaviti velja trgovino EnaA (računalniška trgovina; http://www.enaa.com), ki je dobila najvišjo oceno, in to brez pripomb, kar pomeni, da zadosti vsem varnostnim zahtevam. Poleg tega kot edina slovenska spletna trgovina uporablja 2048-bitni RSA ključ, ki zagotavlja najvišjo raven varnosti. Prav tako je pomembna ugotovitev, da v omenjenem segmentu ne beležimo nobene trgovine, kjer bi nakup zaradi varnostnih razlogov odsvetovali. Preostalih 30 trgovin (75 %) je dobilo zadržano priporočilo nakupa, ker omogočajo zgolj naročanje preko interneta. Kljub vsemu bi pričakovali manjši delež informacijsko »amaterskih« trgovin v segmentu računalništva.

7.15 Razno

V omenjeni segment smo umestili trgovine, ki jih ni bilo mogoče umestiti v druge kategorije. Vsega skupaj smo analizirali 3 trgovine, med katerimi sta 2 dobili oceno »zadržan« in 1 pozitivno oceno. To je trgovina UNICEF (voščilnice, majice; http://www.unicef.si), ki uporablja eksterni plačilni sistem kastor.eon.si in tako ohranja podobo resne organizacije.

7.16 Storitve

Segment storitev ni reprezentativen, ker vsebuje zgolj 2 analizirani trgovini. Je pa zanimiv, ker nakazuje trgovanje z znanjem, ki nima materialne oblike. Prva analizirana trgovina Epravnik (pravne storitve; http://www.epravnik.com), se ukvarja s pravnim svetovanjem proti plačilu. Gre za navadno html stran, ki omogočajo naročanje želenih storitev oziroma definiranje pravnih problemov in nam posreduje odgovor po izvršenem plačilu na njihov transakcijski račun. Trgovina si je prislužila oceno »zadržan«, ker ne uporablja varnostnih protokolov, vendar prav tako ne omogoča plačevanja s kreditnimi karticami. Stranke imajo možnost zastavljanja občutljivih vprašanj in zato ocenjujemo, da bi moralo biti za varnost bolje poskrbljeno. Druga analizirana trgovina je Spletaj (spletno učenje; http://www.spletno-ucenje.com), ki proti plačilu nudi možnost učenja z mentorjem ali brez njega. Stran ne vsebuje varnostnih protokolov in si je prislužila oceno »zadržan«.

7.17 Šport

Na področju športa smo analizirali 14 trgovin. Splošna ocena varnosti trgovin v omenjeni kategoriji je nezadovoljiva. Edina svetla izjema je trgovina Lovski mojster (lovska, potapljaška, ribiška oprema; http://www.btc-city.com/lovskimojster), ki je del virtualnega trgovskega centra z odlično varnostjo nakupov. Preostalim 13 trgovinam (93 %) v segmentu smo pripisali zadržano priporočilo nakupa, ker omogočajo zgolj naročanje in plačilo po povzetju.

7.18 Trgovski portali

V Sloveniji imamo 3 virtualne trgovske portale. Pozitivno oceno sta si prislužila 2 portala: Aperio.si (http://www.aperio.si), ki mu do popolnosti manjka še interaktivna nalepka izdajatelja digitalnega potrdila. Drugi portal je Merkur (http://nakup.merkur.si), ki sicer zadovoljivo poskrbi za varnost nakupa, vendar ne omogoča varne prijave v sistem, kar lahko povzroči zlorabo uporabniškega imena in gesla. Tretji portal, Trgovec.net (http://www.trgovec.net), smo ocenili z zadržkom, ker omogoča zgolj internetno naročanje. Varnost nakupov v kategoriji trgovskih portalov ocenjujemo kot nadpovprečno.

7.19 Vrt in dom

Analizirali smo 6 trgovin s področja vrt in dom. Bodečo nežo smo dodelili trgovini Živex (vse za zunanjo ureditev; http://nakup.zivex.si), ki omogoča vnos številke kreditne kartice brez ustrezne zaščite. Nakup v takšni trgovini odsvetujemo. Preostale trgovine (83 %) omogočajo le naročanje, zato smo jih ocenili z oceno »zadržan«. Na splošno je varnost v kategoriji vrt in dom nezadovoljiva.

7.20 Za otroke

Na področju trgovin za otroke smo analizirali 6 trgovin. Varnost nakupa lahko pohvalimo pri dveh, in sicer BabyCenter (vse za nego in rast otrok; http://www.btc-city.com/babycenter) in Panika records (pesmice in pravljice za otroke; http://otroci.panika.com), slednja trgovina žal kljub odlični varnosti ne omogoča plačevanja s kreditnimi karticami. Druge trgovine v omenjenem segmentu omogočajo zgolj naročanje preko interneta in plačilo po povzetju. Statistično gledano je varnost nakupa v segmentu trgovin za otroke nadpovprečna. Pri tem je pomembno, da nobena trgovina ni dobila negativne ocene.

7.21 Živila, pijače

Kategorija živil in pijač je na internetu relativno dobro zastopana, saj smo našteli 15 trgovin. Varnost nakupa je v omenjeni kategoriji podpovprečna. Priznanje in pozitivno oceno zasluži samo najboljši sosed Mercator (http://www.mercator.si/trgovina), ki odlično poskrbi za varnost prijave in nakupa, vendar omogoča vse vrste plačil šele ob dostavi blaga. S tem zagotavlja popolno varnost in eliminira vsakršno zlorabo. Temu navkljub bi zelo cenili možnost plačila preko interneta že ob samem naročilu. Preostale trgovine v segmentu živil in pijač so prejele oceno »zadržan«, ker gre za klasično naročanje preko interneta in plačilo po povzetju.

7.22 Izbor varnih slovenskih e-trgovin

V prejšnjih poglavjih smo obravnavali vse spletne trgovine. V tem poglavju se bomo osredotočili na 15 % vseh trgovin, ki so dobile pozitivno oceno priporočila nakupa. Govorimo o 31 trgovinah, katerih analizo bomo razširili na poslovanje podjetja in preverjanje v iskalnikih. Namen je ugotoviti, katera podjetja stojijo za spletno trgovino in kako so sposobna izpolnjevati svoje obveznosti. S pomočjo iBon (bonitete poslovanja) smo preverili poslovanje, in sicer ustvarjeni promet v letu 2004, število zaposlenih, denarni tok in morebitne blokade transakcijskih računov (tabela 7.1). Na podlagi pridobljenih informacij smo vsako podjetje umestili v kategorijo (majhno, srednje in veliko podjetje). Majhna podjetja imajo do 50

zaposlenih in ustvarijo do 1 mrd SIT prihodkov, srednja podjetja imajo do 250 zaposlenih in do 4 mrd SIT prihodkov. Velika podjetja imajo več kot 250 zaposlenih in preko 4 mrd SIT prihodkov (Žakelj, 2004).

Tabela 7.1: Varne slovenske e-trgovine

Trgovina	Podjetje	Promet v 000 SIT ('04)	Število zaposlenih	Denarni tok v 000 SIT ('04)	Blokada TRR (v 1 letu)	Velikost podjetja
Aroba (audio-video, HIFI, mobilna telefonija, tiskalniki) http://www.btc-city.com/aroba	Aroba d.o.o.	672.580	13	-40.306	NE	majhno
Aurea (naravna kozmetika) http://www.btc-city.com/aurea	Aurea press d.o.o.	95.893	2	3.155	NE	majhno
BabyCenter (vse za nego in rast) http://www.btc-city.com/babycenter	Baby Center d.o.o.	3.269.333	114	253.102	NE	srednje
Benetton (moda za mlade in odrasle) http://www.btc-city.com/benetton	M POINT d.o.o., Domžale	516.574	22	12.113	NE	majhno
COOL PC (hladilni sistemi za računalnike) http://www.cool-pc.org	Fran Lhotka s.p.	35.247	0	\	NE	majhno
Državna založba Slovenije (slovarji, knjige, učbeniki …) http://trgovina.dzs.si	DZS, d.d.	16.184.664	527	1.008.690	NE	veliko
EnaA (računalniška trgovina) http://www.enaa.com	Gambit trade d.o.o.	2.466.994	22	53.976	NE	srednje
Flegis d.o.o. (ustna higiena) http://www.flegis.si	Flegis d.o.o.	292.867	5	15.949	NE	majhno
Fotomarket (digitalni in klasični fotoaparati ter dodatna oprema) http://www.fotomarket.net	Uroš Fabjan s.p.	418.022	11	\	NE	majhno
JACQUELINE Boutique (spalne srajčke) http://www.impel-bohinj.si/shop	Impel d.o.o.	10.782	2	844	NE	majhno
Lovski mojster (lovska, potapljaška, ribiška oprema) https://www.btc-city.com/lovskimojster	Impressum d.o.o. Kočevje	123.946	4	4.328	NE	majhno
Mentek (računalniška trgovina) http://www.btc-city.com/mentek	Mentek d.o.o.	170.275	11	18.129	NE	majhno
Mercator (prodajalna z živili) http://www.mercator.si/trgovina	Mercator d.d.	228.216.856	7280	11.102.224	NE	veliko
Mimovrste (računalniška trgovina) https://www.mimovrste.com	TI, d.o.o.	485.474	6	6.900	NE	majhno
Mladinska.com (knjige, revije na portalu s spletnimi trgovinami Emka.si, Svetknjige.si, Ciciklub.si, Ucbeniki.si) http://www.mladinska.com	MK Založba d.d.	8.544.769	364	738.292	NE	veliko

Trgovina	Podjetje	Promet v 000 SIT ('04)	Število zaposlenih	Denarni tok v 000 SIT ('04)	Blokada TRR (v 1 letu)	Velikost podjetja
NAKUPI.NET (računalniška trgovina, fotografska oprema) http://www.nakupi.net	Frane Kranjec s.p.	113.986	0	\	NE	majhno
Panika records (pesmice in pravljice za otroke) http://otroci.panika.com	Panika d.o.o.	74.135	4	2.231	NE	majhno
PCplus (računalniška trgovina) http://www.powerplus.si	Acord-92 d.o.o.	3.739.177	38	86.048	NE	srednje
Piromarket (pirotehnika) http://www.piromarket.com	Hamex d.o.o.	490.917	8	31.779	NE	majhno
RedRat Store (računalniška trgovina) http://www.redrat-store.com	Jeza&Co. d.n.o.	36.052	0	1.374	NE	majhno
Svetila in žarnice (profesionalna in dekorativna razsvetljava) http://www.svetila.com	Stanko Plestenjak s.p.	6.943	1	\	NE	majhno
TU-TU Telekom (telekomunikacijska oprema) http://tu-tu.telekom.si	Telekom Slovenije d.d.	88.517.263	2118	32.203.974	NE	veliko
UNICEFOVA trgovina (voščilnice, majice …) http://www.unicef.si	UNICEF Slovenija	\	\	\	\	\
Založba Pasadena (slovenska in tuja računalniška literatura) http://www.pasadena.si/knjigarna	Založba Pasadena d.o.o.	132.243	3	8.340	NE	majhno
Založba Rokus (darila) http://www.darila.com	Darila Rokus d.o.o.	171.422	7	4.867	NE	majhno
Založba Rokus (šolska literatura) http://www.knjigarna.com	Založba Rokus d.o.o.	1.244.128	40	59.249	NE	srednje

Vir: iBon, 2005

Tabela 7.1 predstavlja varne e-trgovine, ki imajo vpeljane ustrezne varnostne protokole in poslujejo pozitivno. Med postopkom analize smo izločili trgovini BOF - Building of Fun (novi lepši svet elektronike; http://www.bof.si) in MojaKnjigarna.com (knjigarna; http://www.mojaknjigarna.com), ker sta v letu 2004 ustvarili negativen denarni tok, kar nakazuje potencialne težave poravnavanja svojih obveznosti. Poleg tega smo iz seznama izločili trgovino Mediteranea (vrhunski izdelki za nego; http://www.mediteranea.si), ker je imelo podjetje v zadnjem letu kar 23 dni blokiran transakcijski račun. Na seznamu smo kljub negativnemu denarnemu toku ohranili trgovino Aroba (audio-video, HIFI, mobilna telefonija, tiskalniki; http://www.btc-city.com/aroba), ker podjetje ustvarja pozitivno akumulacijo, negativen denarni tok pa je posledica aktivnih časovnih razmejitev (AČR). Med drugim na seznam nismo uvrstili spletne trgovine Aperio.si (različne blagovne znamke; http://www.aperio.si), ker podjetje posluje šele pol leta in ne razpolagamo s finančnimi podatki.

Zaključek našega sprehoda med slovenskimi spletnimi trgovinami je priporočilo nakupa v zgoraj omenjenih 26 trgovinah (12,3 %). Pri tem naj poudarimo, da je bil analiziran predvsem varnostni vidik in pozitivno poslovanje. Sama ponudba in konkurenčnost trgovine nista bila obravnavana.

8. PREDLOGI ZA IZBOLJŠANJE VARNOSTI E-TRGOVIN

V poglavju o informacijski varnosti smo omenili, da je za dolgoročni obstoj podjetja ključno zaupanje potrošnikov. Zato si podjetja s svojo malomarnostjo ne bi smela privoščiti izgube zaupanja. Primerno varnost lahko zagotovimo na dva načina. Prvi je razvoj spletne trgovine s protokolom SSL, drugi je razvoj navadne spletne trgovine z uporabo eksternega plačilnega sistema.

Prvi način je razvoj spletne trgovine s protokolom SSL. V internet iskalnik vpišemo ključno besedo »*izdelava spletne trgovine*« in na voljo imamo večje število podjetij, ki nudijo omenjeno storitev (npr. domenca.si, inetia.com, asistent.si, multimedija.net, oblikovanje.com, itd.). Za postavitev spletne trgovine moramo registrirati domeno, izdelati spletno trgovino (koda), najeti strežnike za gostovanje, pridobiti digitalno potrdilo in ostalo, kamor uvrstimo enkratne stroške instalacije, vpisa v spletne imenike, prenos znanja o administriranju itd. Na podlagi pridobljenih informacij zaključimo, da je razpon cen zelo velik, vendar nas vzpostavitev spletne trgovine in prvo leto delovanja v povprečju stane 545.000 SIT, vsako nadaljnje leto pa 256.000 SIT; tu so mišljeni predvsem stroški gostovanja, obnovitve digitalnega potrdila in domene. Pri navajanju cen moramo biti previdni, ker ceniki veljajo za standardizirane rešitve. Morebitne dodatne zahteve se plačujejo po urnih postavkah od približno 7.200 SIT (enostavnejša dela) do 34.800 SIT (ekspertna dela).

V raziskavi o varnosti slovenskih spletnih trgovin smo ugotovili, da kar 80 % trgovin deluje na nezavarovanih html straneh, ki s pomočjo navadnih vpisnih obrazcev omogočajo naročanje artiklov in plačevanje po povzetju. Dejansko so ta podjetja že imela nekatere zgoraj omenjene stroške. Če želimo dodati rešitev za varno nakupovanje, moramo pridobiti digitalno potrdilo in prirediti spletne strani (podpora za SSL). Digitalno potrdilo je možno dobiti za 15.000 SIT na leto (http://www.sigen-ca.si), prireditev spletne strani pa je dodatna storitev, ki jo ocenimo na približno 100.000 SIT. Pri nekaterih gostiteljih je potrebno za podporo SSL dodatno plačati in strošek ovrednotimo na 40.000 SIT na leto. Vse skupaj nas v začetku in prvem letu stane 155.000 SIT, vsako nadaljnje leto pa 55.000 SIT. V kolikor je podpora za SSL že vključena v redno gostovanje, je na letni ravni potrebno upoštevati le strošek podaljševanja digitalnega potrdila v višini 15.000 SIT. Vidimo, da je dodatni strošek za obstoječe spletne trgovce relativno nizek. Pri tem je potrebno upoštevati, da trgovec na takšen način pridobi sloves resnega prodajalca, ki mu je mar za zagotavljanje varnosti nakupov.

Druga rešitev za zagotavljanje varnosti spletnega nakupovanja je uporaba eksternega plačilnega sistema. To pomeni, da je spletna trgovina navadna html stran, ki nas ob odločitvi za nakup preusmeri na skrbno varovani strežnik (ponudnik storitve), kjer do konca izpeljemo postopek nakupa. Pri tem je pomembno, da podatki o naši kreditni kartici zaobidejo trgovca in so posredno avtorizirani na banki. Tako je dovolj, da zaupamo ponudniku eksternega plačilnega sistema.

Primer takšnega sistema je Transact-EON, ki preko tehnologije Transact4 podjetja Open Market iz ZDA ponuja celovito rešitev varnega plačevanja preko interneta s kreditnimi karticami. Sistem je vez med avtorizacijskimi centri in spletnimi trgovinami. Za lažje razumevanje ga lahko opišemo kot virtualni POS terminal, ki avtorizacijo plačilnih in kreditnih kartic opravlja v realnem času. Prednost takšne arhitekture je ločevanje vsebine od transakcije. V praksi to pomeni, da spletno trgovino gradimo neodvisno od plačevanja in trgovcu ni potrebno skrbeti za nove plačilne protokole in standarde, ki so v domeni ponudnika takšne storitve. Za varnost in kodiranje podatkov sistem Transact-EON uporablja 128-bitni protokol SSL podjetja VeriSign. Spletni trgovec se lahko odloči za dva različna paketa: paket EON NULL in paket EON MEGAPOS. Prvi nima mesečne naročnine in predvideva zgolj plačevanje transakcijske provizije v višini 5 % od neto vrednosti uspešne transakcije. Drugi paket vključuje mesečno naročnino v višini 15.000 SIT + DDV in transakcijsko provizijo v višini 1 % od neto vrednosti uspešne transakcije. Pri tem ni vključena siceršnja provizija izdajatelja kreditne kartice, ki znaša med 1 % in 5 % (Telemach, 2005).

Podobno storitev ponuja SiOL z rešitvijo eSiOL, ki omogoča trgovcem varen zajem in obdelovanje plačilnih podatkov. Enako kot pri Transact4 tudi pri tej rešitvi vse informacije o plačilu zaobidejo trgovca in so posredovane procesorju plačilnih instrumentov in nadalje banki. Na takšen način trgovec v svojih bazah podatkov ne razpolaga z občutljivimi informacijami. Posledično nepridiprav nima pravega razloga za napad takšne strani. Strežniki v sistemu eSiOL uporabljajo 128-bitni protokol SSL podjetja VeriSign, ki je najbolj znano svetovno podjetje za spletna varnostna vprašanja. Vsa komunikacija med kupci in sistemom eSiOL ter med trgovci in sistemom eSiOL poteka preko varnih kanalov (SiOL, 2005).

Pri analiziranju stroškov spletne trgovine se spontano pojavi primerjava s stroški klasične trgovine. Na spletnih straneh Davčne uprave Republike Slovenije (http://www.gov.si/durs) je navedena minimalna zajamčena plača v bruto višini 122.600 SIT, kar predstavlja za delodajalca bruto strošek v višini 142.339 SIT na mesec. Zaradi variabilnega delovnega časa potrebujemo vsaj dve trgovki, kar na letni ravni znaša približno 4.180.000 SIT (vključujoč regres, potne stroške in prehrano). Poleg tega potrebujemo trgovino. V Ljubljani znašajo najemnine od 15 €/m^2 na mesec (http://www.nepremicnine.net). Predpostavimo 50 m^2 veliko trgovino, kar nas v letu dni stane najmanj 2.160.000 SIT. Poleg tega je potrebno upoštevati še stroške elektrike, ogrevanja, morebitne opreme itn. Na letni ravni imamo za približno 7

milijonov SIT fiksnih stroškov, kar je neprimerno več kot v primeru implementacije varne internet trgovine.

9. SKLEP

V teoretičnem delu magistrske naloge smo podrobno razdelali osnove kriptografije, opisali različne tehnike, algoritme in protokole, ki se uporabljajo v praksi. Teoretični del smo zaključili s predstavitvijo metode za ocenjevanje varnosti e-trgovin z uporabniškega vidika. Sledili so drugi praktični napotki, kako varno pošiljati elektronsko pošto in varno shranjevati podatke na računalniku. V empiričnem delu naloge smo potrdili temeljno hipotezo.

9.1 Glavne ugotovitve teoretičnega dela

Kriptografija je bila v zgodovini izredno zanimiva in skrivnostna, ker je bila večina dela opravljena v tajnosti. Nasprotno danes varnost šifrirnih algoritmov ne temelji na tajnosti, temveč na široki uporabi. Najboljši algoritmi so tisti, ki so poznani množicam in so zato dobro testirani. Dejansko je čas najboljši pokazatelj dobre kriptografske rešitve. Današnja varnost algoritmov temelji na primernem izboru in ustreznem rokovanju s ključi; daljši ključi zagotavljajo višjo raven varnosti.

Zgodovina kriptografije se prične nekaj sto let pred našim štetjem, njen namen pa je bil tajno sporočanje vojaških napotkov. Kasneje v zgodovini se pojavljajo takšne ali drugačne zahteve po varovanju podatkov pred nepooblaščenim dostopom. V začetku so postopek šifriranja izvajali ročno, danes si pomagamo z računalniki, vendar se šifriranje v svojem bistvu ni spremenilo. Pred tridesetimi leti je bil internet tako rekoč privaten. Omejen je bil na majhne računalniške mreže med vladnimi in akademskimi raziskovalci. Varnost so lahko zagotovili že z dobro ključavnico, s katero so zaklenili strojno opremo. Danes je internet »javen« in z njegovo rastjo ter vedno širšo uporabo postaja varnost ključno vprašanje. Pomagamo si z različnimi kriptografskimi algoritmi.

Na najvišji ravni delimo kriptografske algoritme na simetrične in asimetrične. Simetrična kriptografija uporablja enak ključ za šifriranje in dešifriranje sporočil. Poenostavljeno povedano pošiljatelj zaklene škatlo s sporočilom in jo pošlje po pošti. Prejemnik s pomočjo enakega ključa (identična kopija) škatlo odklene in prebere sporočilo. Simetrični algoritmi so zelo varni in hitri v primerjavi z asimetričnimi, vendar imajo pomembno slabost – problem izmenjave ključev. Ključ je potrebno izmenjati na varen način, kar ni vedno lahko. Odgovor ponuja novodobna rešitev v obliki asimetričnih algoritmov. Že ime nakazuje, da pri takšnem načinu ne uporabljamo istega ključa za šifriranje in dešifriranje. Uporabljamo dva ključa v paru, prvega za šifriranje in drugega, različnega, za dešifriranje. Vsak uporabnik ima 2 ključa: skrbno varovanega privatnega in široko dostopnega javnega. Ključa sta med seboj

matematično povezana, vendar privatnega ključa ni možno izračunati iz javnega. Na primer, če želimo poslati zaupno sporočilo osebi X, uporabimo njen javni ključ (dostopen na internetu). Na drugi strani obstaja točno določen skrbno varovani privatni ključ osebe X, ki je matematično povezan z javnim ključem in edini lahko dešifrira sporočilo. Asimetrični algoritmi torej odpravljajo problem izmenjave ključa in zagotavljajo dodatne varnostne rešitve, vendar so v primerjavi s simetričnimi veliko počasnejši in manj varni. V takšni situaciji je težko reči, kateri mehanizmi so boljši. Tako simetrični kot asimetrični imajo svoje prednosti in slabosti. Idealno rešitev ponuja prepletanje obeh. Asimetrične algoritme uporabljamo za šifriranje in izmenjavo tajnega ključa, ki ga nato uporabimo pri simetričnih algoritmih za šifriranje sporočil. Na takšen način zadostimo pomembnejšim varnostnim zahtevam.

Posebno pozornost je potrebno posvečati zadostni dolžini ključa. Povprečen uporabnik ocenjuje kriptografske rešitve predvsem na podlagi dolžine ključa, ki se pri asimetričnih in simetričnih algoritmih bistveno razlikuje. Nič nenavadnega ni javni ključ velikost 1024 bitov, ki na prvi pogled zagotavlja zadovoljivo varnost. Toda primerljiv simetričen ključ ima dolžino približno 90 bitov, kar ni pretirano veliko. Načeloma pravimo, da je zaželena velikost simetričnega ključa 128 bitov, asimetričnega pa 2048 bitov.

9.2 Glavne ugotovitve empiričnega dela

Pri analizi varnosti slovenskih e-trgovin smo prišli do zaključka, da je kar 80 % spletnih trgovin »amaterskih« in jih lahko postavi že povprečen uporabnik računalnikov. Omogočajo navadno naročanje in plačilo po povzetju, kar je podobno kataloški prodaji, ko iz domačega naslonjača z revijo v roki naročimo želeno blago in ga plačamo po povzetju. Takšne spletne trgovine so popolnoma navadne html strani, ki omogočajo »prisluškovanje«. Ker načeloma ne zahtevajo od nas vnosa številke kreditne kartice, ne moremo reči, da so nevarne, vendar na drugi strani ne zagotavljajo diskretnega nakupa. To lahko povzroči kakšno neprijetno situacijo, večje škode pa ne.

Pozornost je potrebno posvetiti trgovinam, ki so bile ocenjene negativno. Beležimo 5 takšnih trgovin (2 %), ki omogočajo vnos številke kreditne kartice brez ustrezne zaščite. Če se omejimo zgolj na 42 spletnih trgovin, ki omogočajo plačevanje s kreditnimi karticami, ugotovimo, da smo zaradi pomanjkljive varnosti kar pri 12 % odsvetovali nakup. To pomeni, da je v povprečju vsaka osma e-trgovina, ki omogoča plačilo s kreditnimi karticami, potencialno nevarna. *S to ugotovitvijo potrdimo zastavljeno hipotezo, ki trdi, da mnoge slovenske spletne trgovine nimajo vgrajenih ustreznih varnostnih protokolov za zagotavljanje varnega nakupovanja preko interneta*. Seveda se je v takšni trgovini možno poslužiti plačila po povzetju in tako eliminirati riziko vnosa številke kreditne kartice. Morda je pri tem še najbolj moteča malomarnost trgovca, ki za varnost svojih strank ne skrbi zadovoljivo. Že zato

bi nakup bojkotirali. Ugotovitve naše raziskave potrjujejo raziskavo evropskega statističnega urada Eurostat, Uporaba interneta v Evropi, kjer se je Slovenija uvrstila na prvo mesto pri vprašanju oziroma problemu varnega plačevanja. Že v uvodu smo omenili, da je 3,7 % kupcev zaznalo pomanjkljivo varnost pri plačevanju preko interneta, medtem ko je bil ta odstotek pri ostalih državah okoli 1,6 (Demunter, 2005).

Ugotovili smo, da vzpostavitev varne spletne trgovine ni pretirano velik strošek za resnega trgovca, ki si želi zaupanja svojih strank. Primerno varnost je možno zagotoviti na dva načina. Prvi je razvoj spletne trgovine s protokolom SSL, drugi je razvoj navadne spletne trgovine z uporabo eksternega plačilnega sistema. Prvi način, uporaba protokola SSL, je relativno enostavna nadgraditev spletne strani, če upoštevamo, da je podjetje večino stroškov vzpostavitve trgovine že realiziralo. Podobno velja za drugo rešitev, uporabo eksternega plačilnega sistema (npr. eSiOL, Transact-EON). Vse, kar potrebujemo, je pogodba s ponudnikom omenjene storitve in ustrezne povezave iz svoje spletne trgovine na skrbno varovani ponudnikov strežnik, kjer stranka do konca izpelje postopek nakupa.

Analizo varnosti slovenskih spletnih trgovin zaključimo z ugotovitvijo, da brez večjih pomislekov priporočamo nakup le v 12,3 % od skupno 212 spletnih trgovin.

10.LITERATURA

1. Acar Tolga, Michener R. John: Risks in Features vs. Assurance. [URL: http://www.csl.sri.com/users/neumann/insiderisks.html], CACM Inside Risks, 08.08.2002.
2. Aniket P. Kate, Prajakta S. Kalekar, Deepti Agrawal: Weak Keys in Diffie-Hellman Protocol. [URL: http://www.it.iitb.ac.in/~praj/acads/netsec/FinalReport.pdf], 15.11.2004.
3. Arikan Onur: »SET« To Pull Down the Insecurity Barrier in Front of E-commerce. [URL: http://www.biznet.com.tr/dokumanlar/Onur_Arikan_GSEC.html], 25.06.2001.
4. Arild H. Ronny. The International Data Encryption Algorithm. [URL: http://www.pasta.cs.uit.no/thesis/html/ronnya/node16.html], 11.11.1998.
5. Ashley Mike: The GNU Privacy Handbook. The Free Software Foundation. [URL: http://www.gnupg.org/gph/en/manual.html], 03.11.2005.
6. Bamford James: The Puzzle Palace: A Report on America's Most Secret Agency. New York : Penguin Books, 1983. 656 str.
7. Barkley John: Symmetric Key Cryptography. [URL: http://csrc.nist.gov/publications/nistpubs/800-7/node208.html], 07.10.1994.
8. Boncella J. Robert: Web Security for E-commerce. Communications of the Association for Information Systems. [URL: http://www.washburn.edu/cas/cis/boncella/inetsec/tutorial/tutorial.htm], volume 4, article 11, 2000.
9. Bone Simon, Castro Matias: A Brief History of Quantum Computing. [URL: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/], 30.10.2005.
10. Brown H. Karen. Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES). [URL: http://csrc.nist.gov/CryptoToolkit/aes/frn-fips197.pdf], 12.01.2002.
11. Castelino Kenneth: 3DES and Encryption. [URL: http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html], 19.10.2005.
12. Chapple Mike: Cryptography basics for infosecurity managers. [URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci936670,00.html], 20.11.2003.
13. Cherowitzo William: Lecture Notes on Classical Cryptology. [URL: http://www-math.cudenver.edu/~wcherowi/courses/m5410/m5410cc.html], 2005.
14. Cocks C. Clifford: A Note on 'Non-secret Encryption'. [URL: http://www.cesg.gov.uk/site/publications/media/notense.pdf], 20.11.1973.
15. Coles Michael: The Basics of Cryptology. [URL: http://www.sqlservercentral.com/columnists/mcoles/thebasicsofcryptology.asp], 10.08.2005.
16. Coppersmith Don: The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development, vol. 38, n. 3, 1994. str. 243–250.

17. Coron Jean-Sebastien, Joye Marc, Naccache David, Paillier Pascal: Universal Padding Schemes for RSA. Advances in Cryptology – CRYPTO2002, Berlin : Springer-Verlag, vol. 2442, 2002. str. 226-241.
18. Daemen Joan, Rijmen Vincent: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Berlin : Springer Verlag, 2002. 255 str.
19. Diffie Whitfield: The first ten years of public-key cryptography. Proceedings of the IEEE, vol. 76, no. 5, 1988. str. 560-577.
20. Eckel George, Steen William: Intranet Working. Indianapolis USA : New Riders Publishing, 1996. 472 str.
21. Ekert Artur: Cracking codes. [URL: http://plus.maths.org/issue34/features/ekert/], 15.03.2005.
22. Fischer J. Michael: Cryptography and Computer Security. [URL: http://zoo.cs.yale.edu/classes/cs467/2005f/course/lectures/ln06.pdf], 20.09.2005.
23. Freier O. Alan, Karlton Philip, Kocher C. Paul: The SSL Protocol Version 3.0. Transport Layer Security Working Group. [URL: http://wp.netscape.com/eng/ssl3/draft302.txt], 18.11.1996.
24. Grabbe J. Orlin: The DES Algorithm Illustrated. [URL: http://www.aci.net/kalliste/des.htm], 14.05.2005.
25. Greene Tim: Forum warns of hidden DDoS legal liability. [URL: http://www.nwfusion.com/archive/2000/108677_10-02-2000.html], Network World, 02.10.2000.
26. Greenstein Marilyn, Feinman M. Todd: Electronic commerce: Security, Risk Management and Control. New York : Irwin McGraw-Hill, 1999. 416 str.
27. Griffin W. Ricky et al.: Business Essentials (4th edition). Torontno : Prentice Hall, 2002. 544 str.
28. Gromov R. Gregory: History of Internet and WWW: The Roads and Crossroads of Internet History. [URL: http://www.netvalley.com/intval1.html], 13.03.2005.
29. Harris Shon: Security Strategies For E-Companies: The Science Of Secrets. [URL: http://infosecuritymag.techtarget.com/articles/july01/columns_logoff.shtml], julij 2001.
30. Harris Shon: CISSP All-in-One Exam Guide (2nd Edition). New York : McGraw-Hill Osborne Media, 2003. 1008 str.
31. Hipschman Ron: The Secret Language. [URL: http://www.exploratorium.edu/ronh/secret/secret.html], 1995.
32. Hontañón J. Ramón: Encryption 101 - The Choices. [URL: http://www.yoyo.org/~levine/docs/crypto.html], 25.10.2005.
33. Houle J. Kevin, Weaver M. George: Trends in Denial of Service Attack Technology v 1.0. New York : CERT Coordination Center, 2001. 21 str.
34. Jakopin Primož: Zgornja meja entropije pri leposlovnih besedilih v slovenskem jeziku. Ljubljana : Fakulteta za elektrotehniko, 1999. 205 str.

35. Jerman Blažič Borka, Klobučar Tomaž, Perše Zoran, Nedeljkovič Dragan: Elektronsko poslovanje na internetu. Ljubljana : GV Založba, 2001. 206 str.
36. Jurišić Aleksandar, Tonejc Jernej: Zasebno življenje javnih ključev. Ljubljana : Monitor. Infomediji, letnik 11, številka 7-8, 2001. str. 45-51.
37. Khalili Aram: Symmetric cryptography. [URL: http://www.cs.umd.edu/~waa/414-F01/symmetric.pdf], oktober 2005.
38. Koblitz Neal: A Course in Number Theory and Cryptography. Graduate Texts in Mathematics (2nd edition). New York : Springer-Verlag, 1994. 235 str.
39. Kozierok M. Charles: IP Security (IPSec) Protocols. [URL: http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm], 20.09.2005.
40. Lai Xuejia, Massey James: A proposal for a New Block Encryption Standard. Advances in Cryptology – EUROCRYPT '92 Proceedings. New York : Springer-Verlag, 1992, str. 389-404.
41. LaQuey Tracy: The Internet Companion: A Beginner's Guide to Global Networking (2nd edition). Boston : Addison-Wesley, 1994. 262 str.
42. Lawrence Elaine, Corbitt Brain: Internet Commerce: Digital Models for Business (2nd edition). New York : John Wiley & Sons, 2000. 360 str.
43. Lycett Andrew: Breaking Germany's Enigma Code in World War Two. [URL: http://www.bbc.co.uk/history/war/wwtwo/enigma_01.shtml], 01.08.2001.
44. McSweeney John: M150 Data, Computing and Information: The Diffie-Hellman Key Exchange Protocol. [URL: http://www.jmcsweeney.co.uk/computing/m150/diffie_hellman.php], 19.11.2005.
45. Miller Greg: Information Hiding: Past, Present, Future. [URL: http://www.unixjunkie.net/crypto.html], 07.04.2005.
46. Nathan Dan, Cebelenski Chris: Visualizing the PGP Web of Trust. Harvard University. [URL: http://www.simson.net/ref/2004/csci_e-170/handouts/final/nathande-ccbelenski_paper.doc], 10.01.2005.
47. Ng Wing, Yang Wen-Chun: Use DES to generate random numbers in C programming language. [URL: http://islab.oregonstate.edu/koc/ece575/04Project1/Ng-Yang/report.pdf], oktober 2005.
48. Oppliger Rolf: Contemporary Cryptography (Artech House Computer Security503). Boston : Artech House Publishers, 2005, 510 str.
49. Palmgren Keith: Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation. [URL: http://www.securitydocs.com/pdf/2978.PDF], 2.2.2005.
50. Pistoia Marco, Nagaratnam Nataraj, Larry Koved, Nadalin Anthony: Enterprise Java™ Security: Building Secure J2EE™ Applications (1st Editon). Boston : Addison-Wesley Professional, 2004, 608 str.
51. Quisquater Jean-Jacques, Koeune Francois: DSA - Security Evaluation of the Signature Scheme and Primitive. [URL:

http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1001_DSA_report.pdf], februar 2002.
52. Ramage Michael: Symmetric Key Encryption. [URL: http://campus.murraystate.edu/tsm/tsm340/encrypt/private.htm], 07.05.2005.
53. Redshaw Kerry: What's So Logical About Boolean Algebra? [URL: http://www.kerryr.net/pioneers/boolean.htm], 1996.
54. Rescorla Eric: Diffie-Hellman Key Agreement Method. [URL: http://www.ietf.org/rfc/rfc2631.txt], junij 1999.
55. Rivest L. Ronald: The RC5 Encryption Algorithm. [URL: http://theory.lcs.mit.edu/~rivest/Rivest-rc5rev.pdf], marec 1997.
56. Rivest Ron, Shamir Adi, Adleman Len: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. [URL: http://theory.lcs.mit.edu/~rivest/rsapaper.pdf], 24.10.2005.
57. Savage Russ, Totherow Mike: Public Key Infrastructure - Tools for trusting electronic records. [URL: http://www.asu.edu/ecure/2001/totherow/index_total.html], 12.10.2001.
58. Schneier Bruce: Description of a New Variable-Length Key, 64-Bit Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop Proceedings. New York : Springer-Verlag, 1994. str. 191-204.
59. Schneier Bruce: Applied Cryptography (2nd Edition). New York : John Wiley & Sons, 1996, 784 str.
60. Schneier Bruce: The 1998 Crypto Year-in-Review. [URL: http://www.schneier.com/essay-015.html], 19.12.1998.
61. Schneier Bruce: Twofish: A New Block Cipher. [URL: http://www.schneier.com/twofish.html], 14.11.2005.
62. Srinivas N. Raghavan: AES: Who won? Discover the results of the Advanced Encryption Standard contest. [URL: http://www.javaworld.com/javaworld/jw-10-2000/jw-1027-aes.html], oktober 2000.
63. Stallings William: Network and Internetwork Security: Principles and Practice. New Jarsey : Prentice Hall, 1995. 462 str.
64. Thorsteinson Peter, Ganesh A. Gnana: .NET Security and Cryptography (1st edition). New Jarsey : Prentice Hall, 2003. 496 str.
65. Wallhoff John: Methods of Encryption. [URL: http://www.cccure.org/Documents/CISSP_Summary_2002/page14.html], april 2002.
66. Wechtersbach Rado, Lokar Matija: Informatika. Ljubljana : Državna založba Slovenije, 1997. 187 str.
67. Workman Sean: Selecting Appropriate Cryptographic Keys. [URL: http://www.primefactors.com/resources/index.cfm?fuseaction=article&rowid=41], 18.01.2005.
68. Wrixon B. Fred: Codes Ciphers & Other Cryptic & Clandestine Communication. Cologne : Könemann Verlagsgesellschaft, 2000, 704 str.

69. Žakelj Luka: Razvoj malih in srednje velikih podjetij v Sloveniji in Evropski uniji. Ljubljana : UMAR, Delovni zvezek 6, 2004. 56 str.

11.VIRI

1. Asistent – zanesljiva rešitev. [URL: http://www.asistent.si], 25.12.2005.
2. Center Vlade RS za informatiko - Overitelj digitalnih potrdil SIGEN-CA. [URL: http://www.sigen-ca.si/], 10.10.2005.
3. Cisco Systems: White Paper: A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite. [URL: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf], 2002.
4. Davčna uprava Republike Slovenije: Minimalna in zajamčena plača. [URL: http://www.gov.si/durs], 26.12.2005.
5. Demunter Christophe: Internet use in Europe: security and trust (Eurostat). [URL: http://epp.eurostat.cec.eu.int/cache/ITY_OFFPUB/KS-NP-05-025/EN/KS-NP-05-025-EN.PDF], 30.06.2005.
6. Digital Signature Standard (DSS) - FIPS PUB 186-2. [URL: http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf], National Institute of Standards and Technology, 27.01.2000.
7. Domenca: Mavrica spletnih rešitev. [URL: http://www.domenca.si], 25.12.2005.
8. EFF - Electronic Frontier Foundation. [URL: http://www.eff.org/], 17.10.2005.
9. Gerber Scientific: What is Mass Customization? [URL: http://www.mass-customization.com/], 16.03.2005.
10. Gordon Lawrence et al.: Computer Crime and Security Survey. San Francisco : Computer Security Institute Publications, 2004.
11. iBON 2005/II - Bonitete poslovanja. Elektronska verzija 5.2.0.199. Novi forum d.o.o. 2005.
12. inetia.com: Spletne storitve. [URL: http://www.inetia.com], 25.12.2005.
13. iSlovar. [URL: http://www.islovar.org/], 2005.
14. Jutla S. Charanjit: Encryption Modes with Almost Free Message Integrity. [URL: http://csrc.nist.gov/CryptoToolkit/modes/workshop1/presentations/slides-jutla/], 10.06.2005.
15. Koch Werner: GnuPG. Free Software Foundation Inc. [URL: http://www.gnupg.org/], 03.11.2005.
16. MediaCrypt. Swiss Encryption Technology - securing content and transmission. [URL: http://www.mediacrypt.com/], 21.10.2005.
17. Merriam-Webster OnLine. [URL: http://www.m-w.com/], 14.08.2005.
18. Multimedija: Internet Design Studio. [URL: http://www.multimedija.net], 25.12.2005.

19. National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. [URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf], 26.11.2001.
20. Nepremičnine.net: Nepremičninski oglasi. [URL: http://www.nepremicnine.net], 26.12.2006.
21. Network Associates: An Introduction to Cryptography. [URL: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf], 1999.
22. Oblikovanje.com: Spletne rešitve. [URL: http://www.oblikovanje.com], 25.12.2005.
23. Onyszko Tomasz: Authentication, Access Control & Encryption. Secure Socket Layer. [URL: http://www.windowsecurity.com/articles/Secure_Socket_Layer.html], 22.06.2004.
24. RIS: Raba interneta v Sloveniji. [URL: http://www.ris.org], 12.12.2005.
25. RSA Security. [URL: http://www.rsasecurity.com/], 01.10.2005.
26. Seifried Kurt: What's in a Name? SSH Communications. [URL: http://www.seifried.org/security/articles/20020414-ssh-name.html], 14.04.2002.
27. SiOL: Varno nakupovanje na internetu. [URL: http://nakupi.siol.net/PravneInformacije.asp], 26.12.2005.
28. Slovar slovenskega knjižnega jezika, Elektronska izdaja, Verzija 1.0. Inštitut za slovenski jezik Frana Ramovša ZRC SAZU in DZS d.d. ter Amebis d.o.o.
29. SRC sistemske integracije: Obračun plač – informativni izračun plače. [URL: http://www.src.si/storitve/opla/izracun.asp], 26.12.2005.
30. Telemach: Poslovne rešitve E-Trgovina. [URL: http://www.telemach.si], 26.12.2005.
31. Thawte: It's a trust thing. [URL: http://www.thawte.com], 25.12.2005.
32. The Prime Pages. Prime Number Research, Records and Resources. [URL: http://primes.utm.edu/], 15.10.2005.
33. VeriSign. [URL: http://www.verisign.com], 25.12.2005.
34. Wikipedia. [URL: http://www.wikipedia.org/], 03.11.2005.
35. Zakon H. Robert: Hobbes' Internet Timeline v8.0. [URL: http://www.zakon.org/robert/internet/timeline/], 14.03.2005.
36. Zimmermann Phil: Creator of PGP. [URL: http://www.philzimmermann.com/EN/background/index.html], 03.11.2005.

12.Slovarček

3DES	Triple DES	simetrični algoritem za šifriranje
ARPA	Advanced Research Projects Agency	nekdanja ameriška vojaška organizacija
AES	Advanced Encryption Standard	simetrični algoritem za šifriranje
ANSI	American National Standards Institute	inštitut za usklajevanje ameriških standardov z drugimi svetovnimi stan.
atbash		prastara tehnika šifriranja
CA	Certificate Authority	overitelj digitalnih potrdil
CBC	Cipher Block Chaining Mode	metoda šifriranja v blokih
CFB	Cipher Feedback Mode	metoda šifriranja v blokih
DES	Data Encryption Standard	simetrični algoritem za šifriranje
DSA	Digital Signature Algorithm	algoritem za digitalno podpisovanje
DSS	Digital Signature Standard	ameriški standard za digitalno podpisovanje
ECB	Electronic Code Book Mode	metoda šifriranja v blokih
ECC	Elliptic Curve Cryptosystem	asimetrični algoritem za šifriranje
EFF	Electronic Frontier Foundation	neprofitna organizacija za ohranjanje svobode govora v digitalnem kontekstu
ETH	Swiss Federal Institute of Technology	univerza s področja kemije, fizike, elektrotehnike in računalniške znanosti
GCHQ	Government Communications Headquarters	britanska obveščevalna služba za informacijsko varnost
GnuPG	GNU Privacy Guard	brezplačno nadomestilo za PGP
graphia	γραφια	pisati
HTTP	Hyper Text Transport Protocol	protokol za prenos spletnih vsebin
HTTPS	Hyper Text Transport Protocol Secure	varen protokol za prenos spletnih vsebin
IDEA	International Data Encryption Algorithm	simetrični algoritem za šifriranje
IETF	Internet Engineering Task Force	neformalna organizacija za razvoj internetnih standardov
IPSec	Internet Protocol Security	standard za zaščitno internetnega protokola
kryptos	κρνπτοσ	skrivati
Man-In-The-Middle Attack		napad posrednika
NBS	National Bureau of Standards	glej NIST
NIST	National Institute of Standards and Technology	inštitut za razvoj in podporo standardov
NSA	U.S. National Security Agency	največja ameriška obveščevalna služba
OFB	Output Feedback Mode	metoda šifriranja v blokih
PGP	Pretty Good Privacy	program za zagotavljanje kriptografske zasebnosti in verodostojnosti
RC5	Rivest Cipher 5	simetrični algoritem za šifriranje
SET	Secure Electronic Transaction	protokol za zaščito transakcij s kreditnimi karticami
SSH	Secure Shell	program za vzpostavitev varne komunikacije (terminal/strežnik)
SSL	Secure Socket Layer	protokol za zagotavljanje varne komunikacije
TLS	Transport Layer Security	protokol za zagotavljanje varne komunikacije
Web Of Trust		mreža zaupanja
XOR	Exclusive OR	logični operator (ekskluzivni ali)

13.Priloge

Tabela 13.1: Pregled varnosti nakupovanja v vseh analiziranih e-trgovinah

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
avtomobilizem	Beta Global (dodatna avto oprema)	http://www.beta-global.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
avtomobilizem	BITEA (pnevmatike)	http://trgovina.lmbitea.si/trg/kum	NE	NE	\	\	\	PROTI	vnos številke kreditne kartice ni zaščiten
avtomobilizem	Euro TRG (pnevmatike)	http://www.e-gume.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
avtomobilizem	Ilbi (pnevmatike)	http://www.ilbi.info	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
avtomobilizem	OLEF (avtodeli)	http://www.olef-sp.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
avtomobilizem	Suzuki Odar (avtomobili, motorna kolesa, oprema)	http://www.trgovec.net/suzuki	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
avtomobilizem	TC Motoshop (motoristična oprema)	http://tc-motoshop.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Creativ (izobraževalni, predstavitveni in promocijski CDROMi)	http://trgovina.creativ.si/creativ	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Čajna Hiša (pravi čaji, čajni pribor in darila)	http://www.cajnahisa.net	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Darila PI (unikatna svetila, nakit, mozaiki, glineni izdelki, slike, dišavne lučke)	http://www.partneridej.si/darila-pi	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Dvorec Trebnik (unikatni, ročno izdelani, naravi in zdravju prijazni izdelki)	http://www.trebnik.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	E shopping center (darila od 0 do 99 let)	http://www.e-shopping-center.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Gimondo (poslovna darila, koledarji, darilni kompleti)	http://www.gimondo.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
darila	Habeco (promocijska in smešna darila)	http://www.habeco.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Moja parfumerija (za ženske, moške, otroke in najstnike)	http://www.parfumerija-darila.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Pivovarna Laško (spominki)	http://prodaja.turisticnodrustvo-lasko.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
darila	Založba Rokus (darila)	http://www.darila.com	\	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	uporablja eksterni plačilni sistem (kastor.eon.si)
elektronika	Aroba (audio-video, HIFI, mobilna telefonija, tisklniki)	http://www.btc-city.com/aroba	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
elektronika	Atom (izdelki, namenjeni zdravju in lepoti, pripomočki za gospodinjstvo)	http://www.atom.si/trgovina	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Biring (avdio-video oprema, biro oprema, tiskalniki, fotokopirni stroji)	http://trgovina.biring.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	BOF - Building of Fun (novi lepši svet elektronike)	http://www.bof.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	manjka interaktivna CA nalepka
elektronika	Conrad (elektronika)	http://www.conrad.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Dobra Trgovina (mobilna telefonija, računalništvo, dodatna oprema)	http://www.dobratrgovina.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Ebatt (baterije)	http://nakup.dspot-on.net/ebatt	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Faraday (klasične in digitalne antene)	http://shop.faraday.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Fonex (antenski in satelitski sistemi, avdio-video oprema in ostala elektronika)	http://www.efonex.com	NE	NE	\	\	\	PROTI	vnos številke kreditne kartice ni zaščiten
elektronika	Fotomedia (telefonija, fotografija, rabljena oprema)	http://trgovina.media-splet.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	GA (gospodinjski aparati in zabavna elektronika)	http://www.gaa.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
elektronika	Gorenje servis (rezervni deli)	http://www.gorenje-servis.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	GSM Park (telefoni, baterije)	http://gsmpark.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Gsm-oprema (baterije in dodatna oprema)	http://www.gsm-oprema.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Inter diskont (raznovrstna orodja)	http://www.interdiskont.si/on-line	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	KROS (audio, video oprema, LCD in DLP projektorji, diaprojektorji)	http://trgovina.kros.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Mi Trade (GSM dodatna oprema)	http://www.mitrade.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Servis E.s.V.A. (montaža, servis, trgovina klasičnih in satelitskih anten)	http://www.servis-esva.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Svetila in žarnice (profesionalna in dekorativna razsvetljava)	http://www.svetila.com	DA	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	brez pripomb
elektronika	Techno trgovina (foto, hi-fi, video, bela tehnika)	http://www.techno-trgovina.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
elektronika	Tehnika.net (svet tehnike)	http://www.tehnika.net	NE	DA	SSL (128-bit)	RSA (1024-bit)	iprom.si	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic); neznan CA
elektronika	TU-TU Telekom (telekomunikacijska oprema)	http://tu-tu.telekom.si	\	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	brez pripomb
erotika	Diskretno.com (erotični nakupi)	http://www.diskretno.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic); veliko besed o diskretnosti
erotika	Intimna (erotični pripomočki, erotično perilo)	http://www.intimna.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
erotika	Sex Trgovina (erotični filmi, pripomočki in darila)	http://www.sextrgovina.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
erotika	Spolna Moč (povečajte svojo velikost in moč)	http://www.spolnamoc.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
erotika	Sponkina erotična trgovina (erotičnimi pripomočki in filmi)	http://erotika.sponka.tv	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
erotika	Venera Shop (erotični artikli)	http://www.venera-shop.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	DigiFot (fotografska oprema in naročanje razvijanja slik)	http://www.digifot.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Digitalni tisk (koledarji za nadaljnje oblikovanje)	http://digitisk.e-nakupi.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Elis Center (štampiljke, vizitke, elektronski tisk)	http://www.elis-center.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Foto Supra (digitalni fotoaparati in dodatna oprema)	http://www.foto-supra.si/trgovina	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Foto video studio Brbre (spletno naročanje izdelave fotografij)	http://www.fotobrbre.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	FotoDigital (digitalni fotoaparati in druga oprema)	http://www.fotodigital.biz	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Fotodiskont (fotografska oprema)	http://www.fotodiskont.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Fotograd (digitalni fotoaparati in ostala oprema)	http://www.fotograd.com/shop	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Fotomarket (digitalni in klasični fotoaparati ter dodatna oprema)	http://www.fotomarket.net	DA	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	brez pripomb
fotografija, grafika	FotoSplet Meditrade (vse potrebno za fotografiranje)	http://trgovina.meditrade.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Fotostudio Center (fotografska oprema in naročanje razvijanja fotografij)	http://www.fotostudiocenter.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Mixi Foto Video (digitalna oprema)	http://www.mixi.tv	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
fotografija, grafika	Stampiljke.net (naročilo štampiljk)	http://www.stampiljke.net	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
fotografija, grafika	Vizitke.net (izdelava vizitk)	http://www.vizitke.net	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
glasba, video	Glasbena Trgovina HILL (glasbena trgovina)	http://www.slomusic.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
glasba, video	Glasbeni Diskont Planet Muzika (glasbena oprema)	http://glasbeni-diskont.planet-muzika.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
glasba, video	Lastra Company (klasični glasbeni instrumenti)	http://www.lastracom.com	NE	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA (-)	prijava ni zaščitena
glasba, video	MUSICMAX (veleprodaja in maloprodaja glasbil in glasbene opreme)	http://www.musicmax.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
glasba, video	Rec-Rec (glasba, filmi)	http://www.rec-rec.com	NE	DA	SSL (128-bit)	RSA (1024-bit)	iprom.si	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic); neznan CA
glasba, video	Siddharta (albumi in drugi artikli povezani s skupino)	http://www.blagajna.com/siddharta	\	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	brez pripomb
glasba, video	Underground Grooves (vinili in oprema za DJ-je)	http://www.underground-grooves.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
kataloška prodaja	BullBoss (kataloška prodaja)	http://www.bullboss.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
kataloška prodaja	JACQUELINE Boutique (spalne srajčke)	http://www.impel-bohinj.si/shop	\	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	uporablja eksterni plačilni sistem (GlobeCharge)
kataloška prodaja	Neckermann (kataloška prodaja)	http://www.neckermann.si	NE	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA (-)	manjka interaktivna CA nalepka; prijava ni zaščitena
kataloška prodaja	Sponkina spletna trgovina (kataloška prodaja)	http://trgovina.sponka.tv	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
kataloška prodaja	Top Shop (fitnes, kuhinjski pripomočki, za zdravje, sam svoj mojster …)	http://www.topshop.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
kataloška prodaja	TV PRODAJA (kataloška prodaja)	http://www.top1.tv	NE	DA	SSL (128-bit)	RSA (1024-bit)	Kupi d.o.o.	PROTI	neznan CA; prijava ni zaščitena

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
knjige, revije	ANTIKA knjigarna & antikvariat (stare in nove knjige)	http://www.antika.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Bukvarna.com (redke knjige)	http://www.bukvarna.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Bukve.net (vzgoja, izobraževanje, psihoterapija, samopomoč …)	http://www.bukve.net	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Čitanka (osnovnošolski učbeniki in delovni zvezki)	http://www.citanka.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Državna založba Slovenije (slovarji, knjige, učbeniki …)	http://trgovina.dzs.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	manjka interaktivna CA nalepka
knjige, revije	Geonavtik (navtična knjigarna)	http://www.geonavtik.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	GV založba (strokovna literatura)	http://www.gvzalozba.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	KAPITAL (poslovna literatura)	http://www.revijakapital.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Mladinska.com (knjige, revije na portalu s spletnimi trgovinami Emka.si, Svet knjige.si, Ciciklub.si, Učbeniki.si)	http://www.mladinska.com	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	manjka interaktivna CA nalepka
knjige, revije	MojaKnjigarna.com (knjigarna)	http://www.mojaknjigarna.com	DA	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	manjka interaktivna CA nalepka
knjige, revije	Ognjišče (knjige z duhovno vsebino)	http://www.ognjisce.si/knjige	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	OM Šiva (knjige ezoterika, filozofija, joga, religije, psihologija …)	http://www.om-ezoterika.sempco.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Prešernova družba (knjige in revije)	http://www.prdr.com	DA	DA	SSL (128-bit)	RSA (512-bit)	Prešernova družba	PROTI	neznan CA, certifikat potekel, prekratek javni ključ (512-bit)
knjige, revije	Skrivnosti sveta (tematske knjige)	http://www.skrivnosti-sveta.com/e-trgovina	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
knjige, revije	Tehniška založba Slovenije (vse njihove publikacije)	http://www.tzs.si/eknjigarna	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Založba Flamingo (računalniška literatura)	http://flamingotrade.si/shop	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
knjige, revije	Založba Pasadena (slovenska in tuja računalniška literatura)	http://www.pasadena.si/knjigarna	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	manjka interaktivna CA nalepka
knjige, revije	Založba Rokus (šolska literatura)	http://www.knjigarna.com	\	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	uporablja eksterni plačilni sistem (kastor.eon.si)
knjige, revije	Založba Tangram (knjige in učbeniki)	http://www.z-tangram.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Aromas Naturales (naravni osvežilci prostora)	http://www.aromas-naturales.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Aurea (naravna kozmetika)	http://www.btc-city.com/aurea	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
lepota in zdravje	daja* (negovalna in dekorativna kozmetika)	http://www.e-daja.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Flegis d.o.o. (ustna higiena)	http://www.flegis.si	\	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	uporablja eksterni plačilni sistem (kastor.eon.si)
lepota in zdravje	Kosmodisk (hrbtenica)	http://www.kosmodisk.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Lekarnar.com (lekarna)	http://www.lekarnar.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	MEDITERANEA (vrhunski izdelki za nego)	http://www.mediteranea.si	\	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	uporablja eksterni plačilni sistem (kastor.eon.si)
lepota in zdravje	Mind Trade (zeliščni negovalni izdelki)	http://www.mindtrade.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Mineralis (za zdravo življenje)	http://www.mineralis.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Moja parfumerija (vrhunska negovalna kozmetika in parfumi)	http://www.parfumerija-darila.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
lepota in zdravje	zdrav.SI (posteljnina)	http://www.zdrav.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Zdravje z naravo (ohranjanje zdravja in dobrega počutja)	http://www.zdravje.biz	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
lepota in zdravje	Zdravje, lepota, vitalnost (naravni izdelki iz Himalajske soli)	http://www.salinae-med.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Alisa (spodnje perilo in dodatki)	http://trgovina.alisa.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Alpina (obutev)	http://www.alpina.si/si/trgovina	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Benetton (moda za mlade in odrasle)	http://www.btc-city.com/benetton	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
oblačila, obutev, nakit	Cocoon Collection (modni nakit)	http://www.cocoon-collection.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Pizdarije (majice z zabavnimi motivi)	http://shop.pizdarije.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Superge.si (obutev)	http://www.superge.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Tarantela (konfekcija)	http://www.tarantela.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
oblačila, obutev, nakit	Zlatarstvo Kragolnik (zlatarna)	http://www.zlatarstvo-kragolnik.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
optika	Optika Medvešek (kontaktne leče)	http://www.optika-medvesek.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
optika	Optimist optika (optični pripomočki)	http://www.optimist-optika.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pirotehnika	On-line Trgovina Veronika (pirotehnika)	http://www.povzarija.net/pirotehnika	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pirotehnika	Piromarket (pirotehnika)	http://www.piromarket.com	\	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	uporablja eksterni plačilni sistem (e.Siol)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
pisarniški material	Črnila (črnila za ponovno polnjenje kartuš)	http://www.crnila.net	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	Mojrefill (črnila za obnovo kartuš)	http://www.mojrefill.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	Pivk (pisarniški stoli in oprema)	http://www.pivk.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	Polnjenje-kartus.com (polnenje kartuš za InkJet tiskalnike)	http://www.polnjenje-kartus.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	PrismaPaper (papir v različnih formatih, nalepke, folije …)	http://www.prismapaper.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	Svet-Črnil.com (črnila, tonerji)	http://www.svet-crnil.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
pisarniški material	Tiskaj.com (pribori za polnjenje kartuš)	http://www.tiskaj.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Alcyone (računalniška trgovina)	http://shop.alcyone.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Colby- IGABIBA (računalniške igre)	http://igabiba.joker.si	NE	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA (-)	prijava ni zaščitena
računalništvo	Comtron (računalniška trgovina)	http://www.com-shop.com	NE	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA (-)	manjka interaktivna CA nalepka; prijava ni zaščitena
računalništvo	COOL PC (hladilni sistemi za računalnike)	http://www.cool-pc.org	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	odlična varnost, žal brez plačevanja s kreditnimi karticami
računalništvo	EGT Computers (računalniška trgovina)	http://www.egt-trgovina.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	EnaA (računalniška trgovina)	http://www.enaa.com	DA	DA	SSL (128-bit)	RSA (2048-bit)	VeriSign	ZA	brez pripomb
računalništvo	Eproteh (računalniška trgovina in ostala elektronika)	http://www.eproteh.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	E-shop trgovina (računalniška trgovina)	http://www.e-shop.si	DA	DA	SSL (128-bit)	RSA (2048-bit)	Fiver	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic); neznan CA

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
računalništvo	Fenix Trade (računalniška trgovina, elektronika, biro tehnika)	http://www.fenix-trade.si	NE	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA (-)	uporablja eksterni plačilni sistem (WorldPay); prijava in naročilo nista zaščitena
računalništvo	FIDO (računalniška trgovina)	http://trgovina.fido.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Game Shop (računalniške igre)	http://www.eurotronic-arts.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Gigaklik (računalniška trgovina)	http://www.gigaklik.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Gorenje Point (računalniška trgovina)	http://point.gorenje.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	IN.PU.T. (računalniška trgovina)	http://www.in-put.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	IZIshop:net (računalniška trgovina)	http://www.izishop.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	JAE d.o.o. (računalniška trgovina)	http://www.jae.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Kreit (računalniška trgovina, kartuše, tonerji)	http://www.kreit.si/trgovina	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	LANinWAN e-Shop (LAN in WAN oprema)	http://www.laninwan.com/e-shop	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Lokacom (računalniški inženiring)	http://www.lokacom.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	trgovina.locacom.si	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic); neznan CA
računalništvo	Mantis+ (računalniške igre)	http://www.mantisplus.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Mentek (računalniška trgovina)	http://www.btc-city.com/mentek	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
računalništvo	Metaling (računalniška trgovina)	http://trgovina.metaling.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
računalništvo	Mimovrste (računalniška trgovina)	https://www.mimovrste.com	DA	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	manjka interaktivna CA nalepka
računalništvo	NAKUPI.NET (računalniška trgovina, fotografska oprema)	http://www.nakupi.net	DA	DA	SSL (128-bit)	RSA (1024-bit)	SIGEN-CA	ZA	odlična varnost, žal brez plačevanja s kreditnimi karticami
računalništvo	Nakupovanje.net (računalniška trgovina, elektronika, biro oprema)	http://www.nakupovanje.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Nore cene (računalniška trgovina)	http://www.norecene.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	OnLine Trgovina (računalniška trgovina, elektronika, bela tehnika)	http://www.online-trgovina.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	PCplus (računalniška trgovina)	http://www.powerplus.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	manjka interaktivna CA nalepka
računalništvo	PcSVET (računalniška trgovina)	http://www.madison-systems.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	PCtrgovina.Info (računalniška trgovina)	http://www.pctrgovina.info	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Pikanet (računalniška trgovina)	http://www.pikanet.net/trgovina	\	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZADRŽAN	manjka interaktivna CA nalepka; manjka zaklenjena kjučavnica
računalništvo	RedRat Store (računalniška trgovina)	http://www.redrat-store.com	DA	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	odlična varnost, žal brez plačevanja s kreditnimi karticami
računalništvo	Robas e-shop (mrežna oprema)	http://eshop.robas.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Rodocomp (računalniška trgovina, biro oprema)	http://www.rodocomp.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Rolan (računalniki, digitalni fotoaparati, videokamere, televizorji, hi-fi)	http://www.rolan.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	SAT-COM (računalniška trgovina)	http://www.satcom-sp.si/shop	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Teal Laško (računalniška trgovina)	http://www.teal.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
računalništvo	Tech trade (računalniška trgovina)	http://www.techtrade.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Tiskalnik.com (inkjet kartuše)	http://www.tiskalnik.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
računalništvo	Trgovina GLUHI.COM (računalniki, audio-video, foto, tiskalniki)	http://www.gluhi.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
razno	Metra Sežana (železnina)	http://www.metra-sezana.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
razno	UNICEFOVA trgovina (voščilnice, majice …)	http://www.unicef.si	\	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	uporablja eksterni plačilni sistem (kastor.eon.si)
razno	ZAVAS (zaščitna oblačila, obutev ...)	http://www.zavas.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZADRŽAN	digitalno potrdilo ni veljavno
storitve	Epravnik (pravne storitve)	http://www.epravnik.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
storitve	SPLETAJ (spletno učenje)	http://www.spletno-ucenje.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Bike Center (kolesa in kolesarska oprema)	http://bike-center.biz	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Budo Shop (borilne veščine)	http://www.budoshop-sp.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Freerider (kolesa in kolesarska oprema)	http://www.freerider-on.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	idsport (kolesa in kolesarska oprema)	http://www.idsport.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Kibuba (gorništvo)	http://www.kibuba.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Lovski mojster (lovska, potapljaška, ribiška oprema)	https://www.btc-city.com/lovskimojster	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
šport	Mini imports (avtomobilske makete)	http://www.mini-imports.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
šport	MR spletna trgovina (plezalna oprema)	http://www.mrclimbing.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	PlayGame (igralne konzole, igre)	http://www.playgame.biz	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Tekos d.o.o. (šahovska trgovina)	http://www.tekos.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Tengo Sporting Goods (tenis in golf oprema)	http://www.tengo.info/shop	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Tennis Technology (športna oprema za tenis)	http://www.condor-lj.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	Velmark d.o.o. (potapljaška oprema)	http://www.potapljanje.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
šport	X3M SHOP (snowboard, kitesurf in wakeboard oprema)	http://www.x3m-shop.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
trgovski portali	Aperio.si (različne blagovne znamke)	http://www.aperio.si	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	manjka interaktivna CA nalepka
trgovski portali	Merkur (trgovski portal)	http://nakup.merkur.si	NE	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA (-)	prijava ni zaščitena
trgovski portali	Trgovec.net (spletni nakupovalni center)	http://www.trgovec.net	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
vrt in dom	eNakupi.com (spletni nakupovalni center)	http://www.enakup.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
vrt in dom	Gospodinjski aparati (gospodinjskimi aparati, čistilna in likalna tehnika)	http://mt.streznik.org/trg	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
vrt in dom	Opara (vrtne kosilnice, motorne žage, kose …)	http://www.opara.si/shop	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
vrt in dom	Vrtnarstvo Celje (vrtnarski material, oprema, cvetje, drevesa …)	http://www.vrtnarstvo-celje.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
vrt in dom	Zavese (senčila)	http://www.zavese.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
vrt in dom	Živex (za zunanjo ureditev)	http://nakup.zivex.si	NE	NE	\	\	\	PROTI	vnos številke kreditne kartice ni zaščiten
za otroke	Aljaž (otroška oprema)	http://www.aljaz.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
za otroke	BabyCenter (vse za nego in rast)	http://www.btc-city.com/babycenter	DA	DA	SSL (128-bit)	RSA (1024-bit)	Thawte	ZA	možno le plačilo z MasterCard
za otroke	Otroci.org (programi za otroke)	http://www.otroci.org/trgovina	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
za otroke	Panika records (pesmice in pravljice za otroke)	http://otroci.panika.com	\	DA	SSL (128-bit)	RSA (1024-bit)	Equifax	ZA	odlična varnost, žal brez plačevanja s kreditnimi karticami
za otroke	Pikapolonica.com (vse za otroka)	http://www.pikapolonica.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
za otroke	Sonček (igrače, otroška oprema in drugi pripomočki)	http://www.soncek.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Bimed (suho sadje)	http://www.bimed.si/trgovina	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	BoFrost (zamrznjene jedi)	http://shop.bofrost-adria.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	E-nakup dodatkov k prehrani (dodatna in športna prehrana)	http://zdravje.biz	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	eVino (ponudba slovenskih vin)	http://www.wineslove.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	FerMedica (čebelarstvo s tradicijo)	http://www.fermedica-sp.si	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Fitness Shop (športna prehrana)	http://www.fitness-shop-online.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Hiška Dobrot (izdelki iz kontrolirane ekološke pridelave)	http://www.trgovina.hiskadobrot.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Kalček (naravna hrana in aromakultura)	http://www.kalcek.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

PODROČJE	TRGOVINA (opis)	URL	VARNA PRIJAVA	VAREN NAKUP	PROTOKOL	JAVNI KLJUČ	CA	PRIPOROČILO NAKUPA	OPOMBA
živila, pijače	Mercator (prodajalna z živili)	http://www.mercator.si/trgovina	DA	DA	SSL (128-bit)	RSA (1024-bit)	VeriSign	ZA	vse vrste plačil omogočajo šele ob prevzemu blaga
živila, pijače	mojaPrehrana.com (prehrambeni dodatki)	http://www.mojaprehrana.com	NE	DA	SSL (128-bit)	RSA (1024-bit)	mojportal.com	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Profitnes on-line (proteini, preparati za hujšanje …)	http://www.sportna-prehrana.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	VeselePapige (vse za papige)	http://www.veselepapige.com	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Vinogradništvo Fabijan (spletna prodaja vin)	http://www.vino-fabijan.com	\	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	ZOO Market Preis (za živali - hrana in ostali pripomočki)	http://www.zoomarketpreis.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)
živila, pijače	Zoo-Doget.si (za živali - hrana, podlage, posipi, ležišča, šamponi …)	http://zoo.doget.si	NE	NE	\	\	\	ZADRŽAN	zgolj naročanje (ni varovanja, ni plačilnih kartic)

Tabela 13.2: Področje ocenjevanih e-trgovin po parametru »priporočilo nakupa«

Štej od TRGOVINA (opis)	**PRIPOROČILO NAKUPA**				**Skupna vsota**
PODROČJE	**PROTI**	**ZA**	**ZA (-)**	**ZADRŽAN**	
avtomobilizem	1 (14 %)	/	/	6 (86 %)	**7 (100 %)**
darila	/	1 (10 %)	/	9 (90 %)	**10 (100 %)**
elektronika	1 (5 %)	4 (18 %)	/	17 (77 %)	**22 (100 %)**
erotika	/	/	/	6 (100 %)	**6 (100 %)**
fotografija, grafika	/	1 (7 %)	/	13 (93 %)	**14 (100 %)**
glasba, video	/	1 (14 %)	1 (14 %)	5 (71 %)	**7 (100 %)**
kataloška prodaja	1 (17 %)	1 (17 %)	1 (17 %)	3 (50 %)	**6 (100 %)**
knjige, revije	1 (5 %)	5 (26 %)	/	13 (68 %)	**19 (100 %)**
lepota in zdravje	/	3 (23 %)	/	10 (77 %)	**13 (100 %)**
oblačila, obutev, nakit	/	1 (13 %)	/	7 (88 %)	**8 (100 %)**
optika	/	/	/	2 (100 %)	**2 (100 %)**
pirotehnika	/	1 (50 %)	/	1 (50 %)	**2 (100 %)**
pisarniški material	/	/	/	7 (100 %)	**7 (100 %)**
računalništvo	/	7 (18 %)	3 (8 %)	30 (75 %)	**40 (100 %)**
razno	/	1 (33 %)	/	2 (67 %)	**3 (100 %)**
storitve	/	/	/	2 (100 %)	**2 (100 %)**
šport	/	1 (7 %)	/	13 (93 %)	**14 (100 %)**
trgovski portali	/	1 (33 %)	1 (33 %)	1 (33 %)	**3 (100 %)**
vrt in dom	1 (17 %)	/	/	5 (83 %)	**6 (100 %)**
za otroke	/	2 (33 %)	/	4 (67 %)	**6 (100 %)**
živila, pijače	/	1 (7 %)	/	14 (93 %)	**15 (100 %)**
Skupna vsota	**5 (2 %)**	**31 (15 %)**	**6 (3 %)**	**170 (80 %)**	**212 (100 %)**

Tabela 13.3: Deleži različnih overiteljev digitalnih potrdil med varnimi e-trgovinami

Overitelj	**število**	**delež**
Thawte	18	49 %
VeriSign	9	24 %
Equifax	9	24 %
SIGEN-CA	1	3 %
Skupaj	**37**	**100 %**